3

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-344623

(43)Date of publication of application : 29.11.2002

(51)Int.Cl. H04M 3/42
G06F 1/00
G06F 12/14
G06F 13/00
G06F 15/00
H04M 1/00
H04M 3/487

(21)Application number : 2001-142361

(22)Date of filing : 11.05.2001

(71)Applicant : NTT DOCOMO INC

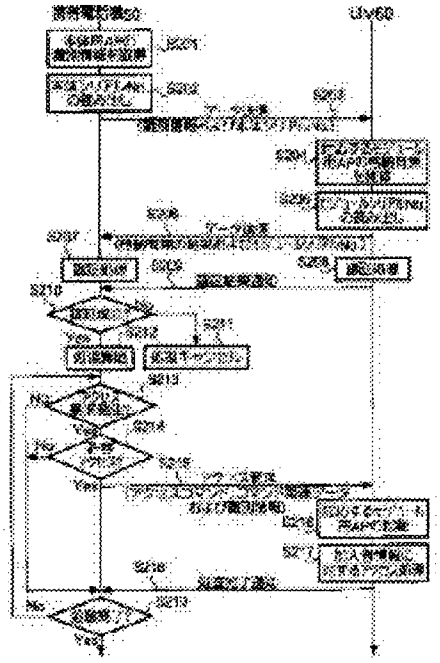
(72)Inventor : TAKAHASHI KAZUHIKO
MURASE ATSUSHI
AZUMA AKIHIRO
NODA CHIE
FURUSE MASAHIRO
UEDA MAKOTO
WAKABAYASHI TATSUAKI
HIRAMATSU TAKAO

(54) ACCESS METHOD, COMMUNICATION TERMINAL, USER IDENTIFICATION MODULE, PROVIDING METHOD FOR PROGRAM, AND TRANSMITTER

(57)Abstract:

PROBLEM TO BE SOLVED: To enable to access to a resource at the outside of a communication terminal except a download source of a program according to the program obtained via a network while ensuring the security.

SOLUTION: A mobile phone 50 and a UIM(User Identity Module) 60 authenticate both a main body use AP (Application Program) and a module AP corresponding to the main body use AP. After authenticating both the programs, a CPU 506 of the mobile phone 50 starts the main body use AP and outputs an access request to subscriber information in the UIM 60 caused in the processing process of the main body use AP to the UIM 60. Upon the receipt of the access request, a CPU 604 of the UIM 60 starts the module use AP corresponding to the main body use AP executed in the mobile phone 50 and reads/writes the subscriber information in response to the access request according to the module use AP.



Japanese Patent Laying-Open No. 2002-344623

[0068] [A-2. Operation of First Embodiment] The operation of the present embodiment will now be described.

<1. Download Processing>

[0069] A portable telephone 50 reads and executes a program of a WWW browser from a ROM 508 when a browsing mode of a WWW page is instructed in accordance with an operational input. Then, based on HTML file data downloaded from a desired contents server 20 through the Internet 30 and a mobile communication network 40, the contents of the WWW page are displayed on a display screen. When a user instructs download of an application program to portable telephone 50 by an operational input while browsing this WWW page, download processing, which will be described below, is started.

[0070] Fig. 9 is a sequence chart illustrating the operation of contents server 20, portable telephone 50, and a UIM 60 in the case of downloading an application program from contents server 20.

[0071] As shown in the drawing, a CPU 506 of portable telephone 50 first transmits a download request to contents server 20 (step S101). This download request contains a command instructing download and information specifying an application program to be downloaded.

[0072] Upon receipt of the download request from portable telephone 50, a CPU 202 of contents server 20 reads the application program in accordance with this download request, from an AP storing region 201a (step S102). The read application program herein refers to a main body AP and a module AP paired with each other, as shown in Fig. 3. Then, CPU 202 downloads these main body AP and module AP to portable telephone 50 in a package (step S103). It is to be noted that the package to be downloaded from contents server 20 to portable telephone 50 may be subjected to compression processing or encryption processing.

[0073] Upon download of the package from contents server 20, CPU 506 of portable telephone 50 performs the following steps S104 to S107 in accordance with a JAM

shown in Fig. 8.

[0074] More specifically, CPU 506 first performs authentication processing of the downloaded package (step S104). This authentication processing is, for example, processing for checking the validity of the downloaded package by an electronic signature, or the like. After this authentication processing, CPU 506 extracts the main body AP and the module AP from the downloaded package (step S105). Then, CPU 506 transmits the module AP and a serial number (main body serial number) of portable telephone 50 read from a serial number storing region 510a, to UIM 60 (step S106). It is to be noted that data to be transmitted from portable telephone 50 to UIM 60 may be subjected to encryption processing.

[0075] CPU 506 also stores the main body AP extracted in the above-described step S106 in an AP storing region 510b in association with a serial number (module serial number) of UIM 60 currently mounted on portable telephone 50 (step S107). It is to be noted that the module serial number is transmitted to portable telephone 50 from UIM 60 when UIM 60 is mounted on portable telephone 50, and stored in a RAM 509.

[0076] Upon receipt of the module AP and the main body serial number from portable telephone 50 in the above-described step S106, a CPU 604 of UIM 60 first activates a loader in OS. Then, in accordance with this loader, CPU 604 stores the module AP in AP storing region 510b in association with the main body serial number (step S108). Thereafter, CPU 604 transmits, to portable telephone 50, an installation completion notification indicating that installation has been completed (step S109). The download processing is thereby terminated.

[0077] As described above, in the download processing, the main body AP and the module AP are downloaded collectively from contents server 20 to portable telephone 50. This can reduce a communication time period and a communication cost required for download.

[0078] <2. Access Management Processing> Fig. 10 is a sequence chart illustrating the operation of portable telephone 50 and UIM 60 in the case where portable telephone 50 makes access to subscriber information in UIM 60. This access

management processing is started when execution of the main body AP is instructed at portable telephone 50.

[0079] CPU 506 of portable telephone 50 first performs the following steps S201 to S203 in accordance with the JAM. More specifically, before executing the instructed main body AP, CPU 506 first acquires identification information (e.g., a file name) of the main body AP instructed to be executed, in order to authenticate this main body AP and the module AP corresponding thereto (step S201). The main body serial number is read from serial number storing region 510a (step S202). Then, CPU 506 transmits the acquired identification information and the main body serial number to UIM 60 (step S203).

[0080] Upon receipt of the identification information and the main body serial number from portable telephone 50, CPU 604 of UIM 60 performs the following steps S204 to S206 in accordance with a card manager in OS. More specifically, in accordance with the received identification information, CPU 604 checks whether or not the module AP corresponding to this main body AP is stored in an AP storing region 605b (step S204). A module serial number is read from a serial number storing region 605a (step S205). Then, CPU 604 transmits the result of presence/absence of storage and the module serial number to portable telephone 50 (step S206).

[0081] Upon receipt of the result of presence/absence of storage and the module serial number from UIM 60, CPU 506 of portable telephone 50 performs authentication processing of the main body AP whose program has been instructed to be executed and the module AP corresponding thereto, in accordance with the JAM (step S207).

[0082] In the present embodiment, the authentication processing of the main body AP and the module AP involves checking two points: whether the module AP corresponding to the main body AP whose program has been instructed to be executed is stored in UIM 60; and whether the current combination of portable telephone 50 and UIM 60 mounted thereon is identical to that of portable telephone 50 and UIM 60 when this main body AP and the module AP are downloaded.

[0083] For the authentication processing shown in the above-described step S207,

CPU 506 checks whether or not the module AP corresponding to the main body AP whose program has been instructed to be executed is stored in UIM 60 in accordance with the result of presence/absence of storage of the module AP transmitted from UIM 60. CPU 506 also compares the module sereal number transmitted from UIM 60 with the module serial number stored in AP storing region 510b in association with the main body AP whose program has been instructed to be executed, thereby checking whether or not the combination of portable telephone 50 and UIM 60 is identical to that when this main body AP and the module AP are downloaded.

[0084] On the other hand, CPU 604 of UIM 60 also performs authentication of the main body AP and the module AP in accordance with the card manager (step S208), and the result of authentication is informed to portable telephone 50 (step S209). Herein, the authentication processing performed in step S208 is similar to that performed at portable telephone 50 side.

[0085] More specifically, CPU 604 checks whether or not the module AP corresponding to the main body AP whose program has been instructed to be executed is stored in UIM 60 in accordance with the result of presence/absence of storage of the module AP distinguished in the above-described step S204. CPU 604 also compares the main body serial number transmitted from portable telephone 50 with the module serial number stored in AP storing region 605b in association with the module AP corresponding to the main body AP whose program has been instructed to be executed, thereby checking whether or not the combination of portable telephone 50 and UIM 60 is identical to that when this main body AP and the module AP are downloaded.

[0086] Upon the authentication processing performed in this manner at both the sides of portable telephone 50 and UIM 60, CPU 506 of portable telephone 50 distinguishes whether or not mutual authentication has been established in accordance with the JAM (step S210). As a result, when mutual authentication has not been established, CPU 506 displays a message showing that authentication has not been established on the screen, and cancels execution of the main body AP (step S211). The access management processing is thereby terminated.

[0087] It is to be noted that the case in which mutual authentication has not been established specifically includes some cases such as where the module AP corresponding to the main body AP whose program has been instructed to be executed is not stored in UIM 60, and where the combination of portable telephone 50 and UIM 60 is different from the combination when this main body AP and the module AP are downloaded.

[0088] On the other hand, when it is distinguished in the above-described step S210 that mutual authentication has been established, CPU 506 first activates, on JavaVM, the main body AP whose program has been instructed to be executed to start processing of the main body AP (step S212). Then, when an access request for subscriber information in UIM 60 occurs during the processing of the main body AP (step S213), CPU 506 distinguishes whether or not this access request is permissible for ensuring security, in accordance with the JAM (step S214).

[0089] Then, when the access request is permitted, CPU 506 transmits, to UIM 60, the access request including the aforementioned access command and command pertinent information, and the identification information of the main body AP (step S215).

[0090] It is to be noted that CPU 506 advances the process into step S219 when no access request has occurred in the above-described step S213, or when the access request has been distinguished as not being permissible in the above-described step S214. Moreover, when the access request has been distinguished as not being permissible in the above-described step S214, it may be configured such thtat a message indicating that an access that is not permissible has occurred is displayed on the screen to stop execution of the main body AP.

[0091] Upon receipt of the access request from portable telephone 50 in the above-described step S215, CPU 604 of UIM 60 specifies a corresponding module AP in accordance with the card manager. Then, CPU 604 executes this module AP on JavaCard VM (step S216).

[0092] Then, in accordance with this module AP, CPU 604 performs access

processing including reading, rewriting, deletion, and the like of subscriber information depending on the access request from portable telephone 50 (step S216). When this access processing is terminated, CPU 604 transmits an access completion notification indicating that the access processing has been completed, to portable telephone 50 (step S218). It is to be noted that, when the access request is reading of subscriber information, the subscriber information as read is included in the access completion notification, and transmitted to portable telephone 50.

[0093] Upon receipt of the access completion notification from UIM 60, CPU 506 of portable telephone 50 distinguishes whether or not the processing of the main body AP is to be terminated (step S219), and when it is not to be terminated, CPU 506 returns the process to the above-described step S213 to continue the processing of the main body AP. When it is to be terminated, the processing of the main body AP is terminated. The access management processing is thereby terminated.

[0094] As described above, according to the the present embodiment, when execution of the main body AP acquired from contents server 20 through Internet 30 is instructed, CPU 506 of portable telephone 50 acquires a module serial number from UIM 60 mounted on portable telephone 50 for comparison with the module serial number associated with the main body AP. CPU 506 thereby distinguishes whether or not the current combination of portable telephone 50 and UIM 60 is identical to the combination of portable telephone 50 and UIM 60 when this main body AP is downloaded.

[0095] Then, when distinguished that the current combination of portable telephone 50 and UIM 60 is identical to the combination of portable telephone 50 and UIM 60 when this main body AP is downloaded, CPU 506 executes the main body AP. Then, during the processing of this main body AP, the main body AP and the corresponding module AP in UIM 60 operate cooperatively, so that access to the subscriber information stored in UIM 60 is made by portable telephone 50.

[0096] That is, execution of the main body AP is canceled and portable telephone 50 cannot make access to the subscriber information in UIM 60 in some cases, such as

where the combination of portable telephone 50 and UIM 60 during execution of the main body AP is identical to that of portable telephone 50 and UIM 60 when this main body AP is downloaded, and where the module AP corresponding to the main body AP is not stored in UIM 60.

[0097] As described, as to execution of the main body AP acquired through the Internet 30, execution is permitted only when the above-described certain conditions hold between portable telephone 50 and UIM 60, so that access to the subscriber information in UIM 60 can be made by portable telephone 50. Therefore, when executing the program acquired through the Internet 30, portable telephone 50 can make access to the subscriber information stored in UIM 60 outside portable telephone 50 in accordance with this program while ensuring security.

[0124] <First Variation> The above first embodiment has described the case in which the main body AP and the module AP are collectively downloaded from contents server 20. However, the procedure of download may be a procedure shown in Fig. 12, for example. Fig. 12 is a sequence chart showing a variation in the case of downloading an application program from contents server 20. It is to be noted that the following will mainly describe a difference from the download processing (see Fig. 9) described in the above embodiment.

[0125] As shown in the drawing, CPU 506 of portable telephone 50 first transmits a download request to contents server 20 (step S301). Upon receipt of the download request from portable telephone 50, CPU 202 of contents server 20 reads, from AP storing region 201a, a main body AP depending on this download request (step S302). Then, CPU 202 downloads the main body AP alone to portable telephone 50 (step S303).

[0126] Upon download of the main body AP from contents server 20, CPU 506 of portable telephone 50 first performs authentication processing of the downloaded main body AP in accordance with the JAM (step S304). This authentication processing is, for example, processing for checking the validity of the downloaded main body AP byan electronic signature, or the like. After this authentication processing, CPU 506

stores the main body AP in AP storing region 510b in association with the module serial number of UIM 60 mounted on portable telephone 50 (step S305). Then, CPU 506 transmits the download request for a module AP corresponding to the stored main body AP to contents server 20 (step S306).

[0127] CPU202 of contents server 20 reads, from AP storing region 201a, a module AP in accordance with the download request from portable telephone 50 (step S307). Then, CPU202 downloads the module AP to portable telephone 50 (step S308).

[0128] Upon download of the module AP from contents server 20, CPU 506 of portable telephone 50 performs authentication processing of the module AP in accordance with the JAM (step S309). Thereafter, CPU 506 transmits the module AP and the main body serial number of portable telephone 50 to UIM 60 in accordance with the JAM (step S310).

[0129] Upon receipt of the module AP and the main body serial number, CPU 604 of UIM 60 stores the module AP in AP storing region 510b in association with the main body serial number, in accordance with the loader in OS (step S311). Thereafter, an installation completion notification is transmitted to portable telephone 50 from UIM 60 (step S312), and the download processing is terminated.

[0130] As described above, the download processing may be configured to download a main body AP and a module AP separately from contents server 20 .

[0131] <Second Variation> The first embodiment and the first variation have described the case in which the main body AP and the module AP are downloaded from contents server 20. However, the present invention is also applicable to the case in which the main body AP and the module AP are distributed to each portable telephone 50 from contents server 20 .

[0132] In this case, contents server 20 has a distribution destination list in which communication addresses (e.g., an IP address, a mail address, etc.) of portable telephone 50 which is a distribution destination are registered. Contents server 20 distributes a main body AP and a module AP to be transmitted, to portable telephone 50 registered in the above-described distribution destination list and UIM 60 mounted

thereon.

[0133] <Third Variation> The first embodiment has described the configuration in which the main body serial number and the module serial number are used in the access management processing for performing authentication processing of the main body AP whose program has been instructed to be executed and the module AP corresponding thereto.

[0134] However, it may be configured such that, when, for example, the main body AP and the module AP are transmitted from contents server 20, identification information different for each package to be transmitted is assigned to both the main body AP and the module AP, and this identification information is used instead of the main body serial number and the module serial number.

[0135] In this case, the main body AP and the module AP as downloaded are stored in AP storing region 510b of portable telephone 50 or AP storing region 605b of UIM 60 in association with the identification information assigned by contents server 20. Then, when performing the authentication processing of the main body AP and the module AP in the access management processing, CPU 506 of portable telephone 50 checks whether or not the identification information associated with the main body AP whose program has been instructed to be executed is identical to the identification information associated with the module AP corresponding to this main body AP.

[0136] Such a configuration enables authentication based on whether or not the main body AP and the module AP are programs downloaded in the same package. It is needless to say that the description of this variation is applicable not only to the case of download but also to the case of distribution.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－344623
（P2002－344623A）
(43)公開日　平成14年11月29日(2002.11.29)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
H04M	3/42		H04M	3/42	E　5B017
G06F	1/00		G06F	12/14	320F　5B076
	12/14	320		13/00	520A　5B085
	13/00	520		15/00	330C　5K015
	15/00	330			330G　5K024

審査請求　未請求　請求項の数23　ＯＬ　（全 22 頁）　最終頁に続く

(21)出願番号　特願2001－142361(P2001－142361)

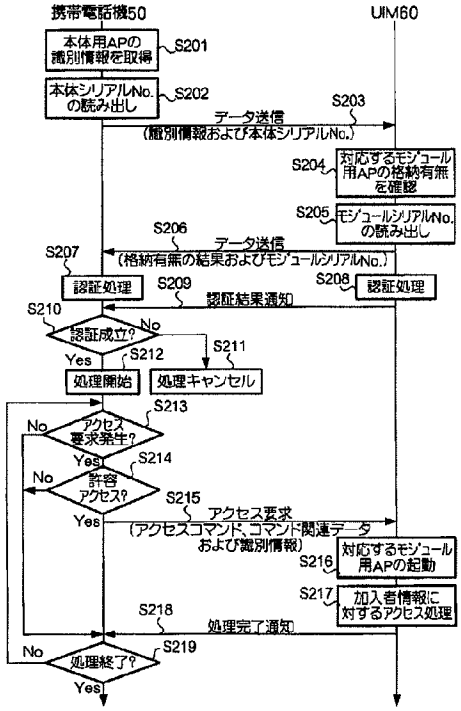
(22)出願日　平成13年５月11日(2001.5.11)

(71)出願人　392026693
株式会社エヌ・ティ・ティ・ドコモ
東京都千代田区永田町二丁目11番１号
(72)発明者　▲高▼橋　和彦
東京都千代田区永田町二丁目11番１号　株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　村瀬　淳
東京都千代田区永田町二丁目11番１号　株式会社エヌ・ティ・ティ・ドコモ内
(74)代理人　100098084
弁理士　川▲崎▼　研二　（外１名）

最終頁に続く

(54)【発明の名称】　アクセス方法、通信端末、ユーザ識別モジュール、プログラムの提供方法および送信装置

(57)【要約】
【課題】　セキュリティを確保しつつ、ネットワークを介して得たプログラムに従って当該プログラムのダウンロード元を除く当該通信端末外のリソースにアクセスできるようにすること。
【解決手段】　携帯電話機５０および当該携帯電話機５０に装着されたＵＩＭ６０では、実行が指示された本体用ＡＰと当該本体用ＡＰに対応するモジュール用ＡＰとの相互認証が行われる。そして、両プログラムが認証された後、携帯電話機５０のＣＰＵ５０６は、本体用ＡＰを起動し、当該本体用ＡＰの処理過程において生じたＵＩＭ６０内の加入者情報に対するアクセス要求をＵＩＭ６０へ出力する。ＵＩＭ６０のＣＰＵ６０４は、アクセス要求を受信すると、携帯電話機５０において実行されている本体用ＡＰに対応するモジュール用ＡＰを起動し、このモジュール用ＡＰに従ってアクセス要求に応じた加入者情報の読み出しや書き込みなどを行う。



1

【特許請求の範囲】

【請求項１】　通信端末が電子機器に記憶されているデータにアクセスする方法であって、

前記通信端末が、ネットワークを介して取得した端末用プログラムを実行する場合に、当該プログラムの実行に伴ってアクセスすることが定められた電子機器と、前記端末用プログラムに対応した電子機器用プログラムを取得した電子機器とが同一であるか否かを判別する第１の過程と、

前記通信端末が、前記第１の過程にて同一であると判別された場合に前記端末用プログラムを実行し、当該プログラムによる処理過程において生じた前記電子機器に対するアクセス要求を当該電子機器に通知する第２の過程と、

前記電子機器が、前記通信端末において実行されている端末用プログラムに対応した電子機器用プログラムに従って、前記第２の過程にて通知されたアクセス要求に応じた処理を実行する第３の過程とを有することを特徴とするアクセス方法。

【請求項２】　前記第１の過程に先立って行われる過程であって、

前記通信端末が、ネットワークを介して端末用プログラムを取得した場合に、当該プログラムに対応した電子機器用プログラムを取得した電子機器から当該電子機器を特定する識別情報を取得して、当該識別情報を前記端末用プログラムと対応付けて記憶する第４の過程をさらに有し、

前記第１の過程では、前記通信端末が、前記端末用プログラムを実行する場合に、当該プログラムの実行に伴ってアクセスすることが定められた電子機器から前記識別情報を取得して、当該識別情報と前記第４の過程にて当該端末用プログラムと対応付けて記憶された識別情報とが同一であるか否かを判別することを特徴とする請求項１記載のアクセス方法。

【請求項３】　前記第１の過程に先立って行われる過程であって、

サーバが、通信端末において実行される端末用プログラムと当該プログラムの実行に伴って電子機器において実行される電子機器用プログラムとを含むパッケージをネットワークを介して送信する場合に、前記パッケージ毎に異なる識別情報を前記端末用プログラムおよび前記電子機器用プログラムの各々に付与して送信する第５の過程と、

前記第５の過程にて送信されたパッケージのうち、前記端末用プログラムを前記通信端末が取得するとともに、前記電子機器用プログラムを前記電子機器が取得する第６の過程とをさらに有し、

前記第１の過程では、前記通信端末が、端末用プログラムを実行する場合に、当該プログラムの実行に伴ってアクセスすることが定められた電子機器から当該端末用プログラムに対応した電子機器用プログラムに付与されている識別情報を取得して、この識別情報と当該端末用プログラムに付与されている識別情報とが同一であるか否かを判別することを特徴とする請求項１記載のアクセス方法。

2

【請求項４】　前記第２の過程は、

前記通信端末が、前記第１の過程にて同一であると判別された場合に前記端末用プログラムを実行し、当該プログラムによる処理過程において前記電子機器に対するアクセス要求が生じた場合に、許容されたアクセスの種類が規定されたアクセス規定データを参照して前記アクセス要求を許可するか否かを決定する第７の過程と、

前記通信端末が前記第７の過程にて許可されたアクセス要求を前記電子機器に通知する第８の過程とを有することを特徴とする請求項１ないし３のいずれか１の請求項に記載のアクセス方法。

【請求項５】　前記電子機器は、前記通信端末に対して着脱自在な、ユーザ情報が記憶されたユーザ識別モジュールであることを特徴とする請求項１ないし４のいずれか１の請求項に記載のアクセス方法。

【請求項６】　電子機器に記憶されているデータにアクセスする通信端末であって、

通信端末において実行可能な端末用プログラムをネットワークを介して受信する受信手段と、

前記受信手段により受信された端末用プログラムを実行する場合に、当該プログラムの実行に伴ってアクセスすることが定められた電子機器と、前記端末用プログラムに対応した電子機器用プログラムを取得した電子機器とが同一であるか否かを判別する判別手段と、

前記判別手段により同一であると判別された場合に前記端末用プログラムを実行する実行手段とを有することを特徴とする通信端末。

【請求項７】　前記受信手段により端末用プログラムを受信した場合に、当該プログラムに対応した電子機器用プログラムを取得した電子機器から当該電子機器を特定する識別情報を取得して、当該識別情報を前記端末用プログラムと対応付けて記憶する識別情報記憶手段をさらに有し、

前記判別手段は、前記端末用プログラムを実行する場合に、当該プログラムの実行に伴ってアクセスすることが定められた電子機器から前記識別情報を取得して、当該識別情報と前記識別情報記憶手段により当該端末用プログラムと対応付けて記憶された識別情報とが同一であるか否かを判別することを特徴とする請求項６記載の通信端末。

【請求項８】　前記受信手段は、通信端末において実行可能な、識別情報が付与されている端末用プログラムをネットワークを介して受信し、

前記判別手段は、前記受信手段により受信された端末用プログラムを実行する場合に、当該プログラムの実行に

伴ってアクセスすることが定められた電子機器から当該端末用プログラムに対応した電子機器用プログラムに付与されている識別情報を取得して、この識別情報と当該端末用プログラムに付与されている識別情報とが同一であるか否かを判別することを特徴とする請求項６記載の通信端末。

【請求項９】　前記実行手段により実行された端末用プログラムによる処理過程において生じた前記電子機器に対するアクセス要求を前記電子機器に送信する送信手段をさらに有することを特徴とする請求項６ないし８のいずれかの請求項に記載の通信端末。

【請求項１０】　前記端末用プログラムに対して許容されたアクセスの種類が記憶されている許容アクセス記憶手段と、

前記実行手段により実行された端末用プログラムによる処理過程において前記電子機器に対するアクセス要求が生じた場合に、前記許容アクセス記憶手段を参照して前記アクセス要求を許可するか否かを決定する決定手段と、

前記決定手段により許可されたアクセス要求を前記電子機器に送信する送信手段とをさらに有することを特徴とする請求項６ないし８のいずれかの請求項に記載の通信端末。

【請求項１１】　電子機器に記憶されているデータにアクセスする通信端末であって、

当該通信端末において実行される端末用プログラムとこのプログラムの実行に伴って当該通信端末によりアクセスされる電子機器において実行される電子機器用プログラムとをネットワークを介して受信する受信手段と、

前記受信手段により受信された端末用プログラムを当該通信端末のメモリに記憶する記憶手段と、

前記受信手段により受信された電子機器用プログラムを前記電子機器に送信する送信手段とを有することを特徴とする通信端末。

【請求項１２】　前記電子機器は、前記通信端末に対して着脱自在な、ユーザ情報が記憶されたユーザ識別モジュールであることを特徴とする請求項６ないし１１のいずれか１の請求項に記載の通信端末。

【請求項１３】　通信端末に対して着脱自在であり、ユーザ情報が記憶されているユーザ識別モジュールであって、

当該ユーザ識別モジュールが装着された通信端末から前記ユーザ情報に対するアクセス要求を受信する受信手段と、

前記通信端末において実行されている端末用プログラムに対応したモジュール用プログラムに従って、前記受信手段により受信されたアクセス要求に応じた前記ユーザ情報に対するアクセス処理を実行する実行手段とを有することを特徴とするユーザ識別モジュール。

【請求項１４】　前記通信端末からの要求に応じて、当該ユーザ識別モジュールを特定する識別情報を前記通信端末に出力する出力手段をさらに有することを特徴とする請求項１３に記載のユーザ識別モジュール。

【請求項１５】　前記通信端末からの要求に応じて、前記通信端末において実行されている端末用プログラムに対応付けられたモジュール用プログラムを特定する特定手段と、

前記特定手段により特定されたモジュール用プログラムに付与されている識別情報を前記通信端末に出力する出力手段とをさらに有することを特徴とする請求項１３に記載のユーザ識別モジュール。

【請求項１６】　通信端末に対して着脱自在であり、ユーザ情報が記憶されているユーザ識別モジュールであって、

当該ユーザ識別モジュールが装着された通信端末から当該通信端末を特定する識別情報と当該ユーザ識別モジュールにおいて実行可能なモジュール用プログラムとを受信し、前記識別情報と前記モジュール用プログラムとを対応付けて記憶する記憶手段と、

当該ユーザ識別モジュールが装着された通信端末から前記識別情報を受信する受信手段と、

前記受信手段により受信された識別情報と前記記憶手段により記憶された識別情報とが同一であるか否かを判別する判別手段と、

前記判別手段による判別結果を前記通信端末に出力する出力手段とを有することを特徴とするユーザ識別モジュール。

【請求項１７】　サーバが、通信端末において実行される端末用プログラムと、当該プログラムの実行に伴って前記通信端末によりアクセスされる電子機器において実行される電子機器用プログラムとをネットワークを介して通信端末に送信する第１の過程と、

前記通信端末が、前記第１の過程にて送信された端末用プログラムと電子機器用プログラムとを受信し、前記端末用プログラムを当該通信端末のメモリに記憶する第２の過程と、

前記通信端末が、前記第２の過程にて受信された電子機器用プログラムを前記電子機器に送信する第３の過程と、

前記電子機器が、前記第３の過程にて送信された電子機器用プログラムを受信し、当該電子機器用プログラムを当該電子機器のメモリに記憶する第４の過程とを有することを特徴とするプログラムの提供方法。

【請求項１８】　前記第２の過程は、

前記通信端末が、前記第１の過程にて送信された端末用プログラムと電子機器用プログラムとを受信する第５の過程と、

前記通信端末が、前記電子機器から当該電子機器を特定する識別情報を取得して、当該識別情報と前記第５の過程にて受信された端末用プログラムとを対応付けて当該

5

通信端末のメモリに記憶する第６の過程とを有することを特徴とする請求項１７記載のプログラムの提供方法。

【請求項１９】　前記第１の過程では、前記サーバが、通信端末において実行される端末用プログラムと、当該プログラムの実行に伴って前記通信端末によりアクセスされる電子機器において実行される電子機器用プログラムとを含むパッケージをネットワークを介して送信する場合に、前記パッケージ毎に異なる識別情報を前記端末用プログラムおよび前記電子機器用プログラムの各々に付与して送信し、

前記第２の過程では、前記通信端末が、前記第１の過程にて送信されたパッケージを受信し、当該パッケージに含まれる端末用プログラムを当該プログラムに対して付与された識別情報とともに当該通信端末のメモリに記憶し、

前記第４の過程では、前記電子機器が、前記第３の過程にて送信された電子機器用プログラムを受信し、この電子機器用プログラムを当該プログラムに対して付与された識別情報とともに当該電子機器のメモリに記憶することを特徴とする請求項１７記載のプログラムの提供方法。

【請求項２０】　前記電子機器は、前記通信端末に対して着脱自在な、ユーザ情報が記憶されたユーザ識別モジュールであることを特徴とする請求項１７ないし１９のいずれか１の請求項に記載のプログラムの提供方法。

【請求項２１】　通信端末において実行される端末用プログラムと、当該プログラムの実行に伴って前記通信端末によりアクセスされる電子機器において実行される電子機器用プログラムとが記憶されている記憶手段と、

通信端末からの指示に応じて、前記記憶手段から読み出した端末用プログラムと電子機器用プログラムとをネットワークを介して前記通信端末に送信する送信手段とを有することを特徴とする送信装置。

【請求項２２】　前記送信手段が前記端末用プログラムと前記電子機器用プログラムとを含んだパッケージを送信する場合に、前記パッケージ毎に異なる識別情報を前記端末用プログラムおよび前記電子機器用プログラムの各々に付与する識別情報付与手段をさらに有することを特徴とする請求項２１に記載の送信装置。

【請求項２３】　前記電子機器は、前記通信端末に対して着脱自在な、ユーザ情報が記憶されたユーザ識別モジュールであることを特徴とする請求項２１または２２に記載の送信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、通信端末が当該通信端末外のリソースにアクセスするために好適なアクセス方法、通信端末、ユーザ識別モジュール、プログラムの提供方法および送信装置に関する。

【０００２】

6

【従来の技術】パーソナルコンピュータやＰＤＡ（Personal Digital Assistant）などの通信端末は、ネットワークに接続されているコンピュータからプログラムをダウンロードし、このプログラムを実行することにより様々な機能を実現することができる。例えば、Java（登録商標）プログラミング言語で記述されたJavaアプレットは、ネットワークを介して通信端末にダウンロードされ、通信端末に組み込まれたブラウザ上で実行されるプログラムである。

【０００３】ところで、インターネットのようなオープンネットワークを利用したデータ通信では、データの改竄、なりすましなどの危険性がある。したがって、このようなオープンネットワークを介して通信端末に提供されたプログラムのセキュリティに関する信頼性を完全に保証することは事実上困難である。

【０００４】以上のようなことから、ネットワークを介して取得したプログラムの実行に関しては、例えば、Javaアプレットの場合、ダウンロードされた通信端末内のごく限られたデータおよびダウンロード元のコンピュータにしかアクセスできないように通信端末においてアクセス制限がなされている。このように、Javaアプレットの実行に際して通信端末は、ダウンロード元のコンピュータ以外の、当該通信端末に接続された周辺機器やネットワークを介して当該通信端末とデータ通信を行うことが可能な他のコンピュータなどにアクセスすることができなかった。

【０００５】

【発明が解決しようとする課題】このようなアクセス制限の仕組みは、セキュリティを確保する上で一定の効果を奏するものの、ネットワークを介して提供されるプログラムに対して様々な動作制限を課すこととなる。すなわち、上記アクセス制限の仕組みは、ネットワークを介して提供されたプログラムにより通信端末における機能の変更や追加などを自由に行えるという本来の利便性を損なう要因であった。

【０００６】一方、ネットワークを介して得たプログラムの実行に際し、何らアクセス制限を設けない場合、前述したデータの改竄、なりすましなどによって、例えば、悪意の第３者により改竄されたプログラムが通信端末にダウンロードされ、当該プログラムの実行に伴う不正なアクセスによる被害が当該通信端末のみならず、他のコンピュータにまで及ぶおそれがあった。

【０００７】本発明は、以上説明した事情に鑑みてなされたものであり、セキュリティを確保しつつ、ネットワークを介して得たプログラムに従って当該プログラムのダウンロード元を除く当該通信端末外のリソースにアクセスすることのできるアクセス方法、通信端末、ユーザ識別モジュール、プログラムの提供方法および送信装置を提供することを目的としている。

【０００８】

【課題を解決するための手段】上記課題を解決するために、この発明は、通信端末が電子機器に記憶されているデータにアクセスする方法であって、前記通信端末が、ネットワークを介して取得した端末用プログラムを実行する場合に、当該プログラムの実行に伴ってアクセスすることが定められた電子機器と、前記端末用プログラムに対応した電子機器用プログラムを取得した電子機器とが同一であるか否かを判別する第１の過程と、前記通信端末が、前記第１の過程にて同一であると判別された場合に前記端末用プログラムを実行し、当該プログラムによる処理過程において生じた前記電子機器に対するアクセス要求を当該電子機器に通知する第２の過程と、前記電子機器が、前記通信端末において実行されている端末用プログラムに対応した電子機器用プログラムに従って、前記第２の過程にて通知されたアクセス要求に応じた処理を実行する第３の過程とを有するアクセス方法を提供する。

【０００９】また、上記アクセス方法において、前記第１の過程に先立って行われる過程であって、前記通信端末が、ネットワークを介して端末用プログラムを取得した場合に、当該プログラムに対応した電子機器用プログラムを取得した電子機器から当該電子機器を特定する識別情報を取得して、当該識別情報を前記端末用プログラムと対応付けて記憶する第４の過程をさらに有し、前記第１の過程では、前記通信端末が、前記端末用プログラムを実行する場合に、当該プログラムの実行に伴ってアクセスすることが定められた電子機器から前記識別情報を取得して、当該識別情報と前記第４の過程にて当該端末用プログラムと対応付けて記憶された識別情報とが同一であるか否かを判別するようにしてもよい。

【００１０】また、上記アクセス方法において、前記第１の過程に先立って行われる過程であって、サーバが、通信端末において実行される端末用プログラムと当該プログラムの実行に伴って電子機器において実行される電子機器用プログラムとを含むパッケージをネットワークを介して送信する場合に、前記パッケージ毎に異なる識別情報を前記端末用プログラムおよび前記電子機器用プログラムの各々に付与して送信する第５の過程と、前記第５の過程にて送信されたパッケージのうち、前記端末用プログラムを前記通信端末が取得するとともに、前記電子機器用プログラムを前記電子機器が取得する第６の過程とをさらに有し、前記第１の過程では、前記通信端末が、端末用プログラムを実行する場合に、当該プログラムの実行に伴ってアクセスすることが定められた電子機器から当該端末用プログラムに対応した電子機器用プログラムに付与されている識別情報を取得して、この識別情報と当該端末用プログラムに付与されている識別情報とが同一であるか否かを判別するようにしてもよい。

【００１１】さらに、上記アクセス方法において、前記第２の過程は、前記通信端末が、前記第１の過程にて同一であると判別された場合に前記端末用プログラムを実行し、当該プログラムによる処理過程において前記電子機器に対するアクセス要求が生じた場合に、許容されたアクセスの種類が規定されたアクセス規定データを参照して前記アクセス要求を許可するか否かを決定する第７の過程と、前記通信端末が前記第７の過程にて許可されたアクセス要求を前記電子機器に通知する第８の過程とを有するようにしてもよい。

【００１２】また、上記アクセス方法において、前記電子機器は、前記通信端末に対して着脱自在な、ユーザ情報が記憶されたユーザ識別モジュールであってもよい。

【００１３】また、上記課題を解決するために、この発明は、電子機器に記憶されているデータにアクセスする通信端末であって、通信端末において実行可能な端末用プログラムをネットワークを介して受信する受信手段と、前記受信手段により受信された端末用プログラムを実行する場合に、当該プログラムの実行に伴ってアクセスすることが定められた電子機器と、前記端末用プログラムに対応した電子機器用プログラムを取得した電子機器とが同一であるか否かを判別する判別手段と、前記判別手段により同一であると判別された場合に前記端末用プログラムを実行する実行手段とを有する通信端末を提供する。

【００１４】また、上記通信端末において、前記受信手段により端末用プログラムを受信した場合に、当該プログラムに対応した電子機器用プログラムを取得した電子機器から当該電子機器を特定する識別情報を取得して、当該識別情報を前記端末用プログラムと対応付けて記憶する識別情報記憶手段をさらに有し、前記判別手段は、前記端末用プログラムを実行する場合に、当該プログラムの実行に伴ってアクセスすることが定められた電子機器から前記識別情報を取得して、当該識別情報と前記識別情報記憶手段により当該端末用プログラムと対応付けて記憶された識別情報とが同一であるか否かを判別するようにしてもよい。

【００１５】また、上記通信端末において、前記受信手段は、通信端末において実行可能な、識別情報が付与されている端末用プログラムをネットワークを介して受信し、前記判別手段は、前記受信手段により受信された端末用プログラムを実行する場合に、当該プログラムの実行に伴ってアクセスすることが定められた電子機器から当該端末用プログラムに対応した電子機器用プログラムに付与されている識別情報を取得して、この識別情報と当該端末用プログラムに付与されている識別情報とが同一であるか否かを判別するようにしてもよい。

【００１６】また、上記通信端末において、前記実行手段により実行された端末用プログラムによる処理過程において生じた前記電子機器に対するアクセス要求を前記電子機器に送信する送信手段をさらに有するようにしてもよい。

【００１７】さらに、上記通信端末において、前記端末用プログラムに対して許容されたアクセスの種類が記憶されている許容アクセス記憶手段と、前記実行手段により実行された端末用プログラムによる処理過程において前記電子機器に対するアクセス要求が生じた場合に、前記許容アクセス記憶手段を参照して前記アクセス要求を許可するか否かを決定する決定手段と、前記決定手段により許可されたアクセス要求を前記電子機器に送信する送信手段とをさらに有するようにしてもよい。

【００１８】また、この発明は、電子機器に記憶されているデータにアクセスする通信端末であって、当該通信端末において実行される端末用プログラムとこのプログラムの実行に伴って当該通信端末によりアクセスされる電子機器において実行される電子機器用プログラムとをネットワークを介して受信する受信手段と、前記受信手段により受信された端末用プログラムを当該通信端末のメモリに記憶する記憶手段と、前記受信手段により受信された電子機器用プログラムを前記電子機器に送信する送信手段とを有する通信端末を提供する。

【００１９】また、上記通信端末において、前記電子機器は、前記通信端末に対して着脱自在な、ユーザ情報が記憶されたユーザ識別モジュールであってもよい。

【００２０】また、上記課題を解決するために、この発明は、通信端末に対して着脱自在であり、ユーザ情報が記憶されているユーザ識別モジュールであって、当該ユーザ識別モジュールが装着された通信端末から前記ユーザ情報に対するアクセス要求を受信する受信手段と、前記通信端末において実行されている端末用プログラムに対応したモジュール用プログラムに従って、前記受信手段により受信されたアクセス要求に応じた前記ユーザ情報に対するアクセス処理を実行する実行手段とを有するユーザ識別モジュールを提供する。

【００２１】また、上記ユーザ識別モジュールにおいて、前記通信端末からの要求に応じて、当該ユーザ識別モジュールを特定する識別情報を前記通信端末に出力する出力手段をさらに有するようにしてもよい。

【００２２】また、上記ユーザ識別モジュールにおいて、前記通信端末からの要求に応じて、前記通信端末において実行されている端末用プログラムに対応付けられたモジュール用プログラムを特定する特定手段と、前記特定手段により特定されたモジュール用プログラムに付与されている識別情報を前記通信端末に出力する出力手段とをさらに有するようにしてもよい。

【００２３】また、この発明は、通信端末に対して着脱自在であり、ユーザ情報が記憶されているユーザ識別モジュールであって、当該ユーザ識別モジュールが装着された通信端末から当該通信端末を特定する識別情報と当該ユーザ識別モジュールにおいて実行可能なモジュール用プログラムとを受信し、前記識別情報と前記モジュール用プログラムとを対応付けて記憶する記憶手段と、当該ユーザ識別モジュールが装着された通信端末から前記識別情報を受信する受信手段と、前記受信手段により受信された識別情報と前記記憶手段により記憶された識別情報とが同一であるか否かを判別する判別手段と、前記判別手段による判別結果を前記通信端末に出力する出力手段とを有するユーザ識別モジュールを提供する。

【００２４】また、上記課題を解決するために、この発明は、サーバが、通信端末において実行される端末用プログラムと、当該プログラムの実行に伴って前記通信端末によりアクセスされる電子機器において実行される電子機器用プログラムとをネットワークを介して通信端末に送信する第１の過程と、前記通信端末が、前記第１の過程にて送信された端末用プログラムと電子機器用プログラムとを受信し、前記端末用プログラムを当該通信端末のメモリに記憶する第２の過程と、前記通信端末が、前記第２の過程にて受信された電子機器用プログラムを前記電子機器に送信する第３の過程と、前記電子機器が、前記第３の過程にて送信された電子機器用プログラムを受信し、当該電子機器用プログラムを当該電子機器のメモリに記憶する第４の過程とを有するプログラムの提供方法を提供する。

【００２５】また、上記プログラムの提供方法において、前記第２の過程は、前記通信端末が、前記第１の過程にて送信された端末用プログラムと電子機器用プログラムとを受信する第５の過程と、前記通信端末が、前記電子機器から当該電子機器を特定する識別情報を取得して、当該識別情報と前記第５の過程にて受信された端末用プログラムとを対応付けて当該通信端末のメモリに記憶する第６の過程とを有するようにしてもよい。

【００２６】また、上記プログラムの提供方法において、前記第１の過程では、前記サーバが、通信端末において実行される端末用プログラムと、当該プログラムの実行に伴って前記通信端末によりアクセスされる電子機器において実行される電子機器用プログラムとを含むパッケージをネットワークを介して送信する場合に、前記パッケージ毎に異なる識別情報を前記端末用プログラムおよび前記電子機器用プログラムの各々に付与して送信し、前記第２の過程では、前記通信端末が、前記第１の過程にて送信されたパッケージを受信し、当該パッケージに含まれる端末用プログラムを当該プログラムに対して付与された識別情報とともに当該通信端末のメモリに記憶し、前記第４の過程では、前記電子機器が、前記第３の過程にて送信された電子機器用プログラムを受信し、この電子機器用プログラムを当該プログラムに対して付与された識別情報とともに当該電子機器のメモリに記憶するようにしてもよい。

【００２７】さらに、上記プログラムの提供方法において、前記電子機器は、前記通信端末に対して着脱自在な、ユーザ情報が記憶されたユーザ識別モジュールであってもよい。

11

【００２８】また、上記課題を解決するために、この発明は、通信端末において実行される端末用プログラムと、当該プログラムの実行に伴って前記通信端末によりアクセスされる電子機器において実行される電子機器用プログラムとが記憶されている記憶手段と、通信端末からの指示に応じて、前記記憶手段から読み出した端末用プログラムと電子機器用プログラムとをネットワークを介して前記通信端末に送信する送信手段とを有する送信装置を提供する。

【００２９】また、上記送信装置において、前記送信手段が前記端末用プログラムと前記電子機器用プログラムとを含んだパッケージを送信する場合に、前記パッケージ毎に異なる識別情報を前記端末用プログラムおよび前記電子機器用プログラムの各々に付与する識別情報付与手段をさらに有するようにしてもよい。

【００３０】また、上記送信装置において、前記電子機器は、前記通信端末に対して着脱自在な、ユーザ情報が記憶されたユーザ識別モジュールであってもよい。

【００３１】

【発明の実施の形態】以下、図面を参照して本発明の実施形態について説明する。なお、各図において共通する部分には、同一の符号が付されている。また、かかる実施形態は本発明の一態様を示すものであり、この発明を限定するものではなく、本発明の範囲で任意に変更可能である。

【００３２】なお、以下の実施形態では、本発明を移動通信システムに適用した場合について説明する。また、以下の実施形態においてアプリケーションプログラムとは、JavaアプレットやJavaアプリケーションなどのJavaプログラミング言語で記述されたアプリケーションプログラムを指す。

【００３３】［Ａ．第１実施形態］

［Ａ－１．第１実施形態の構成］

＜１．移動通信システムの構成＞図１は、この発明の第１実施形態に係るコンテンツサーバ２０、携帯電話機５０およびＵＩＭ（User Identity Module：ユーザ識別モジュール）６０を含む移動通信システム１０の構成を例示するブロック図である。同図に示されるように、移動通信システム１０は、複数のコンテンツサーバ２０と、インターネット３０と、移動通信網４０と、複数の携帯電話機５０と、複数のＵＩＭ６０とを有する。

【００３４】なお、図１においては、図面が煩雑になることを防ぐために、移動通信システム１０を構成する所定のコンテンツサーバ２０、移動通信網４０を構成する所定の基地局４１、移動通信網４０に収容される所定の携帯電話機５０および当該携帯電話機５０に着脱自在な所定のＵＩＭ６０のみが示されている。

【００３５】次に、図１に示された各装置について説明する。コンテンツサーバ２０は、携帯電話機５０に提供する情報を、例えばＨＴＭＬ（HyperText Markup Language）形式のファイルデータとして記憶している。また、コンテンツサーバ２０は、このファイルデータ内でタグにより指定されたJavaアプレットや、Javaアプリケーションなどのプログラムを記憶している。コンテンツサーバ２０は、これらのファイルデータやアプリケーションプログラムをインターネット３０及び移動通信網４０を介して携帯電話機５０に提供する。

12

【００３６】移動通信網４０は、図示を省略した移動パケット通信網および移動電話網を有する。ここで、移動パケット通信網は、パケット通信サービスを提供する網であり、ゲートウェイサーバを介してインターネット３０に接続されている。また、移動電話網は、一般的な移動電話のサービスを提供する網である。また、基地局４１は、移動通信網４０の通信サービスエリア内に多数設置されており、各々の無線セルに在圏する携帯電話機５０と無線通信を行う。

【００３７】携帯電話機５０は、自機が在圏する無線セルをカバーする基地局４１と無線通信を行い、通話サービスやパケット通信サービスを受ける移動機である。この携帯電話機５０は、ＷＷＷ（World Wide Web）ブラウザの機能を有し、このブラウザ機能を利用してコンテンツサーバ２０から提供されるＷＷＷページ（コンテンツ）の内容を液晶画面に表示することができる。また、携帯電話機５０は、ＨＴＭＬファイルデータ内にタグ指定されたJavaアプレットをダウンロードして、このJavaアプレットをWWWブラウザの機能を利用して実行することができる。また、携帯電話機５０は、コンテンツサーバ２０からダウンロードしたJavaアプリケーションを実行することができる。

【００３８】ＵＩＭ６０は、加入者情報が記憶されたモジュールであって、例えば、ＩＣカード（スマートカードとも呼ばれる）の形態を有する。このＵＩＭ６０は、携帯電話機５０に対して着脱自在である。また、このＵＩＭ６０は、マイクロプロセッサを有し、当該モジュール用のアプリケーションプログラムを実行することができる。なお、ＵＩＭ６０に記憶されている加入者情報とは、例えば、このＵＩＭ６０の所有者の電話番号、クレジットカード番号、銀行の口座番号などの個人情報や、所有者の発呼、着呼、通話などの履歴情報、課金情報などのサービス利用情報である。

【００３９】＜２．コンテンツサーバの構成＞図２は、図１に示されたコンテンツサーバ２０のハードウェア構成を例示するブロック図である。同図に示されるように、コンテンツサーバ２０は、メモリ２０１と、ＣＰＵ（Central Processing Unit）２０２と、通信インタフェース２０３とを有し、これらの各部はバス２０４によって接続されている。

【００４０】メモリ２０１には、ＣＰＵ２０２によって実行される各種プログラムや、携帯電話機５０において解釈・実行されるＨＴＭＬファイルデータなどが格納さ

れている。また、このメモリ２０１には、アプリケーションプログラム格納領域２０１ａ（以下、ＡＰ格納領域２０１ａと記載する）が設けられている。このＡＰ格納領域２０１ａには、携帯電話機５０およびこれに装着されたＵＩＭ６０にダウンロードすることが可能なアプリケーションプログラムが格納されている。

【００４１】ここで、ＡＰ格納領域２０１ａに格納されているアプリケーションプログラムとは、携帯電話機５０においてＵＩＭ６０内の加入者情報を参照して実行される、例えば、電子定期券や株のオンライントレード用のプログラムなどである。また、図３に示されるように、ＡＰ格納領域２０１ａに格納されているアプリケーションプログラムは、携帯電話機５０のＣＰＵにより実行される本体用ＡＰと、この本体用ＡＰの実行中にＵＩＭ６０のＣＰＵにより実行されるモジュール用ＡＰとによって構成されている。

【００４２】ＣＰＵ２０２は、メモリ２０１に格納されている各種プログラムを実行することにより、バス２０４を介して接続されている装置各部を制御する。このＣＰＵ２０２は、携帯電話機５０からのダウンロード要求に応じて、この要求に対応するＨＴＭＬファイルデータやアプリケーションプログラムをメモリ２０１から読み出して、通信インタフェース２０３を介して携帯電話機５０に送信する。

【００４３】通信インタフェース２０３は、インターネット３０を介して当該コンテンツサーバ２０と他の装置との間で行われるデータ通信を制御する回路である。

【００４４】＜３．携帯電話機の構成＞図４は、図１に示された携帯電話機５０のハードウェア構成を例示するブロック図である。同図に示されるように、携帯電話機５０は、無線通信部５０１と、操作部５０２と、通話処理部５０３と、表示部５０４と、ＵＩＭインタフェース５０５と、ＣＰＵ５０６と、記憶部５０７とを有し、これらの各部はバス５１１によって接続されている。

【００４５】無線通信部５０１は、アンテナ５０１ａを備え、基地局４１との間で行われる無線データ通信を制御する。この無線通信部５０１は、ＣＰＵ５０６の制御の下、音声データやダウンロード要求などの各種データを搬送波に重畳し、この信号をアンテナ５０１ａから基地局４１に送信する。また、無線通信部５０１は、基地局４１から自機宛てに送られてくる信号をアンテナ５０１ａを介して受信し、これを復調して音声データやＨＴＭＬファイルデータ、アプリケーションプログラムなどを得る。

【００４６】操作部５０２は、数字や文字、操作指示などを入力するための複数のキーを備え、これらのキーの操作に応じた操作信号をＣＰＵ５０６に出力する。通話処理部５０３は、例えば、マイクロフォンやスピーカ、音声処理部などを有し、ＣＰＵ５０６の制御の下、呼接続／切断処理を含む通話処理を行う。表示部５０４は、液晶表示パネルと、この液晶表示パネルの表示制御を行う駆動回路とを有する。ＵＩＭインタフェース５０５は、当該携帯電話機５０に装着されたＵＩＭ６０との間で行われるデータ通信を制御する回路である。

【００４７】記憶部５０７は、ＲＯＭ（Read Only Memory）５０８と、ＲＡＭ（Random Access Memory）５０９と、例えば、ＳＲＡＭ（Static－RAM）やＥＥＰＲＯＭ（Electrically Erasable Programmable Read Only Memory）などの不揮発性メモリ５１０とを有する。

【００４８】ＲＯＭ５０８には、ＣＰＵ５０６によって実行される各種プログラムなどが格納されている。例えば、ＲＯＭ５０８には、携帯電話機５０用のオペレーティングシステム（以下、ＯＳと略称する）やＷＷＷブラウザのプログラム、Javaプログラミング言語で記述されたプログラムを当該携帯電話機５０において実行するためのJava実行環境（以下、ＪＲＥと略称する）のソフトウェアなどが格納されている。

【００４９】ＲＡＭ５０９は、ＣＰＵ５０６のワークエリアとして用いられ、例えば、コンテンツサーバ２０からダウンロードされたＨＴＭＬファイルデータやアプリケーションプログラムなどが一時的に格納される。

【００５０】不揮発性メモリ５１０は、シリアルナンバー格納領域５１０ａと、ＡＰ格納領域５１０ｂとを有する。シリアルナンバー格納領域５１０ａには、携帯電話機５０毎に固有のシリアルナンバー（製造番号）が、例えば工場出荷時に書き込まれる。また、ＡＰ格納領域５１０ｂには、コンテンツサーバ２０からダウンロードされたアプリケーションプログラムのうち本体用ＡＰが格納される。ここで、図５に示されるように、ＡＰ格納領域５１０ｂに格納される本体用ＡＰは、ダウンロードされた時点において当該携帯電話機５０に装着されているＵＩＭ６０のシリアルナンバーと対応付けられて格納される。

【００５１】ＣＰＵ５０６は、記憶部５０７に格納されている各種プログラムを実行することにより、バス５１１を介して接続されている装置各部を制御する。このＣＰＵ５０６は、本実施形態に特有な処理として、後述するダウンロード処理（図９参照）およびアクセス管理処理（図１０参照）を実行する。

【００５２】＜４．ＵＩＭの構成＞図６は、図１に示されたＵＩＭ６０のハードウェア構成を例示するブロック図である。同図に示されるように、ＵＩＭ６０は、外部インタフェース６０１と、ＲＯＭ６０２と、ＲＡＭ６０３と、ＣＰＵ６０４と、ＥＥＰＲＯＭ６０５とを有し、これらの各部はバス６０６によって接続されている。

【００５３】外部インタフェース６０１は、携帯電話機５０との間で行われるデータ通信を制御する回路である。

【００５４】ＲＯＭ６０２には、ＣＰＵ６０４によって実行される各種プログラムなどが格納されている。例え

ば、ＲＯＭ６０２には、ＵＩＭ６０用のＯＳや、Javaプログラミング言語で記述されたプログラムを当該ＵＩＭ６０において実行するためのJavaカード実行環境（以下、ＪＣＲＥと略称する）のソフトウェア、携帯電話機５０から受信したモジュール用ＡＰをＥＥＰＲＯＭ６０５に格納するローダのプログラムがなど格納されている。

【００５５】ＲＡＭ６０３は、ＣＰＵ６０４のワークエリアとして用いられ、例えば、携帯電話機５０から受信したモジュール用ＡＰなどが一時的に格納される。

【００５６】ＥＥＰＲＯＭ６０５は、シリアルナンバー格納領域６０５ａと、ＡＰ格納領域６０５ｂと、加入者情報格納領域６０５ｃとを有する。シリアルナンバー格納領域６０５ａには、ＵＩＭ６０毎に固有のシリアルナンバーが、例えば工場出荷時に書き込まれる。また、ＡＰ格納領域６０５ｂには、携帯電話機５０から受信したモジュール用ＡＰが格納される。ここで、図７に示されるように、ＡＰ格納領域６０５ｂに格納されるモジュール用ＡＰは、このモジュール用ＡＰがダウンロードされた時点において当該ＵＩＭ６０が装着されている携帯電話機５０のシリアルナンバーと対応付けられて格納される。また、加入者情報格納領域６０５ｃには、前述した個人情報やサービス利用情報などの加入者情報が格納されている。

【００５７】ＣＰＵ６０４は、ＲＯＭ６０２やＥＥＰＲＯＭ６０５に格納されている各種プログラムを実行することにより、バス６０６を介して接続されている各部を制御する。このＣＰＵ６０４は、本実施形態に特有な処理として、後述するダウンロード処理（図９参照）およびアクセス管理処理（図１０参照）を実行する。

【００５８】＜５．アプリケーションプログラムの実行環境＞図８は、本体用ＡＰとモジュール用ＡＰの実行環境を例示する模式図である。同図左側に示される機能階層モデルは、携帯電話機５０における本体用ＡＰの実行環境を示すものであり、同図右側に示される機能階層モデルは、ＵＩＭ６０におけるモジュール用ＡＰの実行環境を示すものである。

【００５９】まず、同図左側の本体用ＡＰの実行環境を示す機能階層モデルは、最下層側から上位層に向かって順に、ＯＳ（携帯電話機５０用）と、Javaアプリケーションマネージャ（以下、ＪＡＭと略称する）と、Javaバーチャルマシン（以下、JavaＶＭと略称する）と、複数の本体用ＡＰとを有する。

【００６０】ここで、ＯＳは、携帯電話機５０の基本的な制御を司る機能を有する。ＪＡＭは、各本体用ＡＰの実行に関するセキュリティなどを管理する機能を有する。また、JavaＶＭは、ＪＡＭによる制御の下、本体用ＡＰを実行するための機能を有し、Javaの実行ファイル形式であるバイトコードを携帯電話機５０のＣＰＵ５０６がＯＳを介して解釈可能な命令コードに変換する。Ｊ

ＡＭおよびJavaＶＭは、ＪＲＥに組み込まれており、携帯電話機５０のＲＯＭ５０８に記憶されている。

【００６１】次に、同図右側のモジュール用ＡＰの実行環境を示す機能階層モデルは、最下層側から上位層に向かって順に、ＯＳ（ＵＩＭ６０用）と、Javaカードバーチャルマシン（以下、Java Card ＶＭと略称する）およびローダと、複数のモジュール用ＡＰとを有する。

【００６２】ここで、ＯＳは、ＵＩＭ６０の基本的な制御を司る機能を有する。このＯＳには、ＵＩＭ６０内の各モジュール用ＡＰの格納有無を確認したり、携帯電話機５０から受信したアクセス要求をどのモジュール用ＡＰに引き渡すのかを判断するカードマネージャの機能が含まれる。また、Jav a Card ＶＭは、モジュール用ＡＰを実行するための機能を有し、Javaのバイトコードを ＵＩＭ６０のＣＰＵ６０４がＯＳを介して解釈可能な命令コードに変換する。このJava Card ＶＭは、ＪＣＲＥに組み込まれており、ＵＩＭ６０のＲＯＭ６０２に記憶されている。また、ローダは、携帯電話機５０から受信したデータやプログラムをＥＥＰＲＯＭ６０５にインストールする機能を有し、ＯＳ上で実行される。

【００６３】なお、ＵＩＭ６０において各モジュール用ＡＰは、Java Card ＶＭの仕様により、原則として当該アプリケーションが管理する加入者情報にしかアクセスできない構成となっている。

【００６４】次に、この図８に基づいて、携帯電話機５０からＵＩＭ６０内の加入者情報に対してアクセスする場合の動作を説明する。携帯電話機５０のＣＰＵ５０６は、本体用ＡＰによる処理過程においてＵＩＭ６０内の加入者情報に対するアクセス要求が生じると、まず、ＪＡＭに従ってこのアクセス要求がセキュリティを確保する上で許容されるものであるか否かを判断する。その結果、アクセス要求が許容された場合、このアクセス要求がJavaＶＭによりＣＰＵ５０６で解釈可能な命令コードに変換される。

【００６５】ここで、アクセス要求には、アクセスコマンドとコマンド関連データとが含まれる。アクセスコマンドとは、例えば、読み出し、書き換え、削除など、加入者情報に対するアクセスの種類を示すものである。また、コマンド関連データとは、例えば、書き換えるデータを指定する情報や書き換え用のデータ、読み出すデータを指定する情報などである。ＣＰＵ５０６は、ＯＳに従ってこのアクセスコマンドとコマンド関連データとを含むアクセス要求をＵＩＭインタフェース５０５経由でＵＩＭ６０に送信する。

【００６６】ＵＩＭ６０のＣＰＵ６０４は、外部インタフェース６０１を介してアクセス要求を受信すると、まず、ＯＳ内のカードマネージャに従ってアクセス要求を引き渡すモジュール用ＡＰを特定する。次いで、このモジュール用ＡＰがJava CardＶＭ上において起動される。そして、ＣＰＵ６０４は、このモジュール用ＡＰに

従って、アクセス要求に応じた加入者情報に対する読み出しや書き換え、削除などのアクセス処理を実行する。

【００６７】なお、図８左側に示された本体用ＡＰの実行環境を示す機能階層モデルにおいて、JavaＶＭは、ＫＶＭ（K Virtual Machine）などであってもよい。以上が本実施形態に係る移動通信システム１０の構成である。

【００６８】［Ａ－２．第１実施形態の動作］次に、本実施形態の動作について説明する。

＜１．ダウンロード処理＞

【００６９】携帯電話機５０は、操作入力に応じてWWWページの閲覧モードが指示された場合に、ＲＯＭ５０８からWWWブラウザのプログラムを読み出して実行する。そして、所望のコンテンツサーバ２０からインターネット３０および移動通信網４０を介してダウンロードされたＨＴＭＬファイルデータに基づいて、表示画面にWWWページの内容を表示する。ユーザがこのWWWページの閲覧中に携帯電話機５０に対してアプリケーションプログラムのダウンロードを操作入力により指示すると、以下に説明するダウンロード処理が開始される。

【００７０】図９は、コンテンツサーバ２０からアプリケーションプログラムをダウンロードする場合の、コンテンツサーバ２０、携帯電話機５０およびＵＩＭ６０の動作を例示するシーケンスチャートである。

【００７１】同図に示されるように、まず、携帯電話機５０のＣＰＵ５０６は、ダウンロード要求をコンテンツサーバ２０に送信する（ステップＳ１０１）。このダウンロード要求には、ダウンロードを指示するコマンドとダウンロードするアプリケーションプログラムを指定する情報とが含まれる。

【００７２】コンテンツサーバ２０のＣＰＵ２０２は、携帯電話機５０からダウンロード要求を受信すると、このダウンロード要求に応じたアプリケーションプログラムをＡＰ格納領域２０１ａから読み出す（ステップＳ１０２）。ここで読み出されるアプリケーションプログラムとは、図３に示されたように、ペアとして対応付けられている本体用ＡＰおよびモジュール用ＡＰである。そして、ＣＰＵ２０２は、この本体用ＡＰおよびモジュール用ＡＰを１つのパッケージとして携帯電話機５０にダウンロードする（ステップＳ１０３）。なお、コンテンツサーバ２０から携帯電話機５０にダウンロードされるパッケージに対しては、圧縮処理や暗号化処理が施されていてもよい。

【００７３】携帯電話機５０のＣＰＵ５０６は、コンテンツサーバ２０からパッケージをダウンロードすると、図８に示されたＪＡＭに従って、以下のステップＳ１０４～Ｓ１０７の処理を行う。

【００７４】すなわち、まず、ＣＰＵ５０６は、ダウンロードしたパッケージに対する認証処理を行う（ステップＳ１０４）。この認証処理は、例えば、電子署名などによって、ダウンロードしたパッケージの正当性を確認する処理である。この認証処理の後、ＣＰＵ５０６は、ダウンロードされたパッケージから本体用ＡＰおよびモジュール用ＡＰを取り出す（ステップＳ１０５）。そして、ＣＰＵ５０６は、モジュール用ＡＰとシリアルナンバー格納領域５１０ａから読み出した当該携帯電話機５０のシリアルナンバー（本体シリアルナンバー）とをＵＩＭ６０に送信する（ステップＳ１０６）。なお、携帯電話機５０からＵＩＭ６０に送信されるデータに対しては、暗号化処理が施されていてもよい。

【００７５】また、ＣＰＵ５０６は、上記ステップＳ１０６において取り出した本体用ＡＰを、現時点において携帯電話機５０に装着されているＵＩＭ６０のシリアルナンバー（モジュールシリアルナンバー）と対応付けてＡＰ格納領域５１０ｂに格納する（ステップＳ１０７）。なお、モジュールシリアルナンバーは、ＵＩＭ６０が携帯電話機５０に装着された時点でＵＩＭ６０から携帯電話機５０に送信され、ＲＡＭ５０９に格納されている。

【００７６】一方、ＵＩＭ６０のＣＰＵ６０４は、上記ステップＳ１０６において携帯電話機５０からモジュール用ＡＰおよび本体シリアルナンバーを受信すると、まず、ＯＳ内のローダを起動する。そして、ＣＰＵ６０４は、このローダに従って当該モジュール用ＡＰを本体シリアルナンバーと対応付けてＡＰ格納領域５１０ｂに格納する（ステップＳ１０８）。この後、ＣＰＵ６０４は、インストールが完了したことを示すインストール完了通知を携帯電話機５０に送信する（ステップＳ１０９）。これにより当該ダウンロード処理が終了する。

【００７７】以上説明したようにダウンロード処理では、本体用ＡＰおよびモジュール用ＡＰがコンテンツサーバ２０から携帯電話機５０に一括してダウンロードされる。したがって、ダウンロードに要する通信時間や通信コストを低減することができる。

【００７８】＜２．アクセス管理処理＞図１０は、携帯電話機５０がＵＩＭ６０内の加入者情報にアクセスする場合の、携帯電話機５０およびＵＩＭ６０の動作を例示するシーケンスチャートである。このアクセス管理処理は、携帯電話機５０において本体用ＡＰの実行が指示された場合に開始される。

【００７９】携帯電話機５０のＣＰＵ５０６は、まず、ＪＡＭに従って、以下のステップＳ２０１～Ｓ２０３の処理を行う。すなわち、ＣＰＵ５０６は、指示された本体用ＡＰを実行する前に、この本体用ＡＰとこれに対応するモジュール用ＡＰの認証を行うために、まず、実行が指示された本体用ＡＰの識別情報（例えば、ファイル名）を取得する（ステップＳ２０１）。また、シリアルナンバー格納領域５１０ａから本体シリアルナンバーを読み出す（ステップＳ２０２）。そして、ＣＰＵ５０６は、取得した識別情報および本体シリアルナンバーをＵ

ＩＭ６０に送信する（ステップＳ２０３）。

【００８０】ＵＩＭ６０のＣＰＵ６０４は、携帯電話機５０から識別情報および本体シリアルナンバーを受信すると、ＯＳ内のカードマネージャに従って、以下のステップＳ２０４～Ｓ２０６の処理を行う。すなわち、ＣＰＵ６０４は、受信した識別情報に従って、この本体用ＡＰに対応するモジュール用ＡＰがＡＰ格納領域６０５ｂに格納されているか否かを確認する（ステップＳ２０４）。また、シリアルナンバー格納領域６０５ａからモジュールシリアルナンバーを読み出す（ステップＳ２０５）。そして、ＣＰＵ６０４は、格納有無の結果およびモジュールシリアルナンバーを携帯電話機５０に送信する（ステップＳ２０６）。

【００８１】携帯電話機５０のＣＰＵ５０６は、ＵＩＭ６０から格納有無の結果およびモジュールシリアルナンバーを受信すると、ＪＡＭに従い、プログラムの実行が指示された本体用ＡＰとこれに対応するモジュール用ＡＰとの認証処理を行う（ステップＳ２０７）。

【００８２】本実施形態において、本体用ＡＰとモジュール用ＡＰとの認証処理とは、実行が指示された本体用ＡＰに対応するモジュール用ＡＰがＵＩＭ６０に格納されていること、および現時点における携帯電話機５０とこれに装着されたＵＩＭ６０の組み合わせが、この本体用ＡＰおよびモジュール用ＡＰをダウンロードした時の携帯電話機５０とＵＩＭ６０の組み合わせと同一であること、の二点を確認することである。

【００８３】ＣＰＵ５０６は、上記ステップＳ２０７に示す認証処理として、ＵＩＭ６０から送信されたモジュール用ＡＰの格納有無の結果に従って、実行が指示された本体用ＡＰに対応するモジュール用ＡＰがＵＩＭ６０に格納されているか否かを確認する。また、ＣＰＵ５０６は、ＵＩＭ６０から送信されたモジュールシリアルナンバーと、実行が指示された本体用ＡＰと対応付けられてＡＰ格納領域５１０ｂに格納されているモジュールシリアルナンバーとを比較することにより、携帯電話機５０とＵＩＭ６０の組み合わせがこの本体用ＡＰおよびモジュール用ＡＰをダウンロードした時の組み合わせと同一であるか否かを確認する。

【００８４】一方、ＵＩＭ６０のＣＰＵ６０４においても、カードマネージャに従い、本体用ＡＰとモジュール用ＡＰとの認証が行われ（ステップＳ２０８）、認証結果が携帯電話機５０に通知される（ステップＳ２０９）。ここで、上記ステップＳ２０８において行われる認証処理は、携帯電話機５０側で行われる認証処理と同様である。

【００８５】すなわち、ＣＰＵ６０４は、上記ステップＳ２０４において判別したモジュール用ＡＰの格納有無の結果に従って、プログラムの実行が指示された本体用ＡＰに対応するモジュール用ＡＰが当該ＵＩＭ６０に格納されているか否かを確認する。また、ＣＰＵ６０４

は、携帯電話機５０から送信された本体シリアルナンバーと、実行が指示された本体用ＡＰに対応するモジュール用ＡＰに対応付けられてＡＰ格納領域６０５ｂに格納されているモジュールシリアルナンバーとを比較することにより、携帯電話機５０とＵＩＭ６０の組み合わせがこの本体用ＡＰおよびモジュール用ＡＰをダウンロードした時の組み合わせと同一であるか否かを確認する。

【００８６】このようにして携帯電話機５０とＵＩＭ６０との双方で認証処理が行われた後、携帯電話機５０のＣＰＵ５０６は、ＪＡＭに従い、相互認証が成立したか否かを判別する（ステップＳ２１０）。その結果、相互認証が成立しなかった場合、ＣＰＵ５０６は、認証が不成立であった旨のメッセージを画面表示し、本体用ＡＰの実行をキャンセルする（ステップＳ２１１）。また、これにより当該アクセス管理処理が終了する。

【００８７】なお、相互認証が成立しなかった場合とは、具体的には、プログラムの実行が指示された本体用ＡＰに対応するモジュール用ＡＰがＵＩＭ６０に格納されていなかった場合や、携帯電話機５０とＵＩＭ６０の組み合わせがこの本体用ＡＰおよびモジュール用ＡＰをダウンロードした時の組み合わせと異なる場合などである。

【００８８】一方、ＣＰＵ５０６は、上記ステップＳ２１０において相互認証が成立したと判別した場合には、まず、実行が指示された本体用ＡＰをJavaＶＭ上において起動し、当該本体用ＡＰの処理を開始する（ステップＳ２１２）。次いで、ＣＰＵ５０６は、本体用ＡＰによる処理過程においてＵＩＭ６０内の加入者情報に対するアクセス要求が発生すると（ステップＳ２１３）、ＪＡＭに従って、このアクセス要求がセキュリティを確保する上で許容されるものであるのか否かを判別する（ステップＳ２１４）。

【００８９】そして、ＣＰＵ５０６は、アクセス要求が許容された場合、前述したアクセスコマンドおよびコマンド関連情報と、当該本体用ＡＰの識別情報とを含むアクセス要求をＵＩＭ６０に送信する（ステップＳ２１５）。

【００９０】なお、ＣＰＵ５０６は、上記ステップＳ２１３においてアクセス要求が発生していない場合や、上記ステップＳ２１４においてアクセス要求が許容されないものであった場合には、ステップＳ２１９の処理に移行する。また、上記ステップＳ２１４においてアクセス要求が許容されないものであった場合には、許容不可のアクセスが発生したことを示すメッセージを画面表示し、本体用ＡＰの実行を中止する構成としてもよい。

【００９１】ＵＩＭ６０のＣＰＵ６０４は、上記ステップＳ２１５において携帯電話機５０からアクセス要求を受信すると、カードマネージャに従い、対応するモジュール用ＡＰを特定する。そして、ＣＰＵ６０４は、Java Card ＶＭ上においてこのモジュール用ＡＰを実行する

（ステップＳ２１６）。

【００９２】次いで、ＣＰＵ６０４は、このモジュール用ＡＰに従い、携帯電話機５０からのアクセス要求に応じた加入者情報に対する読み出しや書き換え、削除などのアクセス処理を実行する（ステップＳ２１６）。このアクセス処理が終了すると、ＣＰＵ６０４は、アクセス処理が完了したことを示すアクセス完了通知を携帯電話機５０に送信する（ステップＳ２１８）。なお、アクセス要求が加入者情報の読み出しであった場合は、読み出された加入者情報がアクセス完了通知に含まれて携帯電話機５０に送信される。

【００９３】携帯電話機５０のＣＰＵ５０６は、ＵＩＭ６０からアクセス完了通知を受信すると、本体用ＡＰの処理を終了するか否かを判別し（ステップＳ２１９）、終了でなければ上記ステップＳ２１３に戻り、本体用ＡＰの処理を継続する。また、終了であれば、本体用ＡＰの処理を終了する。これにより当該アクセス管理処理が終了する。

【００９４】以上説明したように本実施形態によれば、携帯電話機５０のＣＰＵ５０６は、コンテンツサーバ２０からインターネット３０を介して取得した本体用ＡＰの実行が指示されると、当該携帯電話機５０に装着されたＵＩＭ６０からモジュールシリアルナンバーを取得し、本体用ＡＰに対応付けられたモジュールシリアルナンバーと比較する。これによりＣＰＵ５０６は、現時点における携帯電話機５０とＵＩＭ６０の組み合わせが、この本体用ＡＰをダウンロードした時点における携帯電話機５０とＵＩＭ６０の組み合わせと同一であるか否かを判別する。

【００９５】そして、ＣＰＵ５０６は、現時点における携帯電話機５０とＵＩＭ６０の組み合わせが、この本体用ＡＰをダウンロードした時点における携帯電話機５０とＵＩＭ６０の組み合わせと同一であると判別した場合に、本体用ＡＰを実行する。そして、この本体用ＡＰによる処理過程においては、本体用ＡＰおよびこれに対応するＵＩＭ６０内のモジュール用ＡＰが連携して動作することにより、携帯電話機５０からＵＩＭ６０に格納されている加入者情報へのアクセスが行われる。

【００９６】つまり、本体用ＡＰの実行時における携帯電話機５０とＵＩＭ６０の組み合わせがこの本体用ＡＰをダウンロードした時点における携帯電話機５０とＵＩＭ６０の組み合わせと異なる場合や、本体用ＡＰに対応するモジュール用ＡＰがＵＩＭ６０に格納されていなかった場合などは、本体用ＡＰの実行がキャンセルされ、携帯電話機５０は、ＵＩＭ６０内の加入者情報にアクセスすることができない。

【００９７】このように、インターネット３０を介して取得した本体用ＡＰの実行については、携帯電話機５０とＵＩＭ６０との間で上述した一定の条件が成立した場合にのみ実行が許可され、携帯電話機５０からＵＩＭ６０内の加入者情報へのアクセスが可能となる。したがって、携帯電話機５０は、インターネット３０を介して取得したプログラムの実行に際し、セキュリティを確保しつつ、このプログラムに従って当該携帯電話機５０外の、ＵＩＭ６０に格納されている加入者情報にアクセスすることができる。

【００９８】［Ａ－３．具体的な適用例］以下に本発明を適用したアプリケーションプログラムの概要を説明する。

＜１．電子定期券アプリケーション＞本発明を電子定期券のアプリケーションプログラムに適用した場合について説明する。この場合、ＵＩＭ６０には、加入者情報としてさらに、利用者氏名や利用区間、有効期間などの定期券情報が格納されている。また、携帯電話機５０は、例えば、ＨｏｍｅＲＦ（Home Radio Frequency）やBluetooth（登録商標）などにより改札に設置された利用者の通過許可を判断する制御装置との間で近距離の無線通信を行う近距離無線通信部をさらに有する。

【００９９】改札を通過する際、携帯電話機５０およびこれに装着されたＵＩＭ６０では、電子定期券用の本体用ＡＰとモジュール用ＡＰとの相互認証が行われる。そして、相互認証が成立した後、携帯電話機５０のＣＰＵ５０６は、電子定期券用の本体用ＡＰを起動し、改札に設置された制御装置からの信号を受信する。次いで、ＣＰＵ５０６は、この信号の受信に応じて、定期券情報の読み出しを指示するアクセス要求をＵＩＭ６０に送信する。

【０１００】ＵＩＭ６０のＣＰＵ６０は、アクセス要求の受信に応じて電子定期券用のモジュール用ＡＰを起動し、当該モジュール用ＡＰに従ってＵＩＭ６０内の定期券情報を読み出して携帯電話機５０に送信する。携帯電話機５０のＣＰＵ５０６は、ＵＩＭ６０から定期券情報を受信すると、この定期券情報を近距離無線通信部により制御装置に送信する。そして、改札に設置された制御装置は、受信した定期券情報に従って、この携帯電話機５０を所持する利用者の通過許可を決定する。

【０１０１】＜２．決済アプリケーション＞次に、本発明を決済処理のアプリケーションプログラムに適用した場合について説明する。この場合、ＵＩＭ６０には、加入者情報としてクレジットカード番号や銀行の口座番号などの決済に使用する決済使用情報が格納されている。

【０１０２】インターネット３０に接続されているサーバやＰＯＳ（Point Of Sales）などの端末と通信を行って商品の売買契約を行い、代金支払いの決済を行う場合、携帯電話機５０およびこれに装着されているＵＩＭ６０では、決済処理用の本体用ＡＰとモジュール用ＡＰとの相互認証が行われる。そして、相互認証が成立した後、携帯電話機５０のＣＰＵ５０６は、決済処理用の本体用ＡＰを起動して決済方法の選択メニューを画面表示し、ユーザに選択を促す。これに応じてユーザは、キー

操作により決済方法を選択する。次いで、ＣＰＵ５０６は、ユーザにより選択された決済方法に該当する決済使用情報の読み出しを指示するアクセス要求をＵＩＭ６０に送信する。

【０１０３】ＵＩＭ６０のＣＰＵ６０は、アクセス要求の受信に応じて決済処理用のモジュール用ＡＰを起動し、当該モジュール用ＡＰに従って該当する決済使用情報を読み出して携帯電話機５０に送信する。携帯電話機５０のＣＰＵ５０６は、ＵＩＭ６０から決済使用情報を受信すると、この決済使用情報を液晶画面に表示する。そして、ユーザにより暗証番号情報などがキー操作によって入力され、最終的な決済の指示が決定されると、携帯電話機５０は、暗証番号情報などを含んだ決済使用情報を暗号化してＰＯＳなどの相手先装置に送信する。これにより相手先装置と決済センタや金融機関の決済サーバとの間で商品の売買契約に伴う決済処理が行われる。

【０１０４】［Ｂ．第２実施形態］上記第１実施形態では、携帯電話機５０から当該携帯電話機５０に装着されたＵＩＭ６０内の加入者情報に対してアクセスする場合について説明した。本実施形態では、携帯電話機からパーソナルコンピュータなどの電子機器に記憶されたデータに対してアクセスする場合について説明する。

【０１０５】なお、本実施形態において、上記第１実施形態と共通する部分については同一の符号を使用するものとする。また、上記第１実施形態と共通する部分についてはその説明を省略するものとする。

【０１０６】［Ｂ－１．第２実施形態の構成］図１１は、第２実施形態に係る携帯電話機５５のハードウェア構成を例示するブロック図である。同図において上記第１実施形態の携帯電話機５０と異なるのは、ＵＩＭインタフェース５０５の代わりに赤外線通信部５５０が設けられ、この赤外線通信部５５０を介して当該携帯電話機５５が電子機器７０とデータ通信を行うことが可能な点である。

【０１０７】赤外線通信部５５０は、赤外線通信（例えば、ＩｒＤＡ（InfraRed Data Association）規格に従った通信）により電子機器７０との間で行われるデータ通信を制御する。

【０１０８】電子機器７０は、例えば、パーソナルコンピュータやＰＤＡなどであり、上述した赤外線通信機能を有している。また、この電子機器７０は、Javaプログラミング言語で記述されたプログラムの実行環境（ＪＲＥ）を有している。ここで、この電子機器７０におけるJavaプログラムの実行環境は、上記第１実施形態におけるＵＩＭ６０の場合と異なり、Java Card ＶＭの代わりにＪＡＭとJavaＶＭとを有する。また、この電子機器７０内のメモリには、例えば、この電子機器７０の所有者の氏名やクレジットカード番号などの個人情報が格納されている。

【０１０９】本実施形態においてコンテンツサーバ２０から携帯電話機５５および電子機器７０にダウンロードされるアプリケーションプログラムは、携帯電話機５５のＣＰＵ５０６により実行される端末用ＡＰと、電子機器７０のＣＰＵにより実行される電子機器用ＡＰとによって構成されている。また、電子機器用ＡＰは、コンテンツサーバ２０から携帯電話機５５を経由して電子機器７０にダウンロードされる。

【０１１０】また、本実施形態における携帯電話機５５は、アクセス先の電子機器を特定する情報として、コンテンツサーバ２０からダウンロードした電子機器用ＡＰを電子機器７０へ送信した際に、この電子機器７０とのデータ通信に使用した当該携帯電話機５５の入出力ポート番号を端末用ＡＰと対応付けて不揮発性メモリ５１０に格納する。また、不揮発性メモリ５１０のＡＰ格納領域５１０ｂには、電子機器用ＡＰをダウンロードした電子機器７０から取得した当該電子機器７０のシリアルナンバーが端末用ＡＰと対応付けられて格納される。

【０１１１】［Ｂ－２．第２実施形態の動作］次に、本実施形態の動作について説明する。本実施形態において携帯電話機５５および電子機器７０は、上記第１実施形態において説明したダウンロード処理（図９参照）と同様の処理を実行する。そして、このダウンロード処理において携帯電話機５５からの操作入力によって指定されたコンテンツサーバ２０内の端末用ＡＰおよび電子機器用ＡＰは、インターネット３０を介して携帯電話機５５にダウンロードされる。

【０１１２】携帯電話機５５は、まず、電子機器用ＡＰを送信する電子機器７０から当該電子機器７０のシリアルナンバーを赤外線通信部５５０経由で取得して、当該シリアルナンバーとダウンロードした端末用ＡＰとを対応付けてＡＰ格納領域５１０ｂに格納する。また、携帯電話機５５は、電子機器７０とのデータ通信に使用した当該携帯電話機５５の入出力ポート番号を、この端末用ＡＰの処理過程においてアクセスする電子機器の特定情報として、端末用ＡＰと対応付けて不揮発性メモリ５１０に格納する。

【０１１３】次いで、携帯電話機５５は、シリアルナンバー格納領域５１０ａに格納されている自機のシリアルナンバーを読み出して、当該シリアルナンバーとダウンロードした電子機器用ＡＰとを赤外線通信部５５０により電子機器７０に送信する。電子機器７０では、受信した携帯電話機５５のシリアルナンバーと電子機器用ＡＰとを対応付けてメモリに格納する。

【０１１４】そして、携帯電話機５５および電子機器７０は、上記第１実施形態において説明したアクセス管理処理（図１０参照）と同様の処理を実行し、プログラムの実行が指示された端末用ＡＰおよびこれに対応する電子機器用ＡＰの相互認証を行う。そして、相互認証された端末用ＡＰおよび電子機器用ＡＰが連携して動作することにより、携帯電話機５５から電子機器７０内の個人

情報に対するアクセス処理が行われる。

【０１１５】より具体的に説明すると、まず、ユーザは、アクセス先となる電子機器７０を操作して、当該電子機器７０が携帯電話機５５と赤外線通信を行うことが可能な状態とする。次いで、ユーザは、携帯電話機５５に対して、端末用ＡＰの実行を指示する操作入力を行う。これに応じて携帯電話機５５のＣＰＵ５０６は、実行が指示された端末用ＡＰと対応付けて不揮発性メモリ５１０に格納している入出力ポート番号（アクセス先の電子機器を特定する情報）を読み出す。

【０１１６】次いで、携帯電話機５５は、読み出した入出力ポート番号に従って赤外線通信部５５０を選択し、当該携帯電話機５５と赤外線通信を行うことが可能な状態にある電子機器を特定するための呼出し信号を赤外線通信部５５０から送信する。そして、携帯電話機５５は、この呼出し信号に対して応答信号を返信してきた電子機器７０を特定する。

【０１１７】次いで、携帯電話機５５のＣＰＵ５０６は、特定した電子機器７０から当該電子機器７０のシリアルナンバーを赤外線通信部５５０経由で取得し、端末用ＡＰに対応付けられているシリアルナンバーと比較する。これによりＣＰＵ５０６は、現時点において携帯電話機５５と赤外線通信を行っている電子機器７０がこの端末用ＡＰとペアになる電子機器用ＡＰをダウンロードした電子機器７０であるか否かを判別する。

【０１１８】そして、ＣＰＵ５０６は、携帯電話機５５と赤外線通信を行っている電子機器７０が実行指定された端末用ＡＰとペアになる電子機器用ＡＰをダウンロードした電子機器７０であると判別した場合に、端末用ＡＰを実行する。この端末用ＡＰによる処理過程においては、端末用ＡＰおよびこれに対応する電子機器７０内の電子機器用ＡＰが連携して動作することにより、携帯電話機５５から電子機器７０のメモリに格納されている加入者情報へのアクセスが行われる。

【０１１９】つまり、端末用ＡＰの実行時において、携帯電話機５５と赤外線通信を行っている電子機器７０が端末用ＡＰとペアになる電子機器用ＡＰをダウンロードした電子機器７０と異なる場合や、この電子機器７０に端末用ＡＰに対応する電子機器用ＡＰが格納されていなかった場合などは、端末用ＡＰの実行がキャンセルされ、携帯電話機５５は、電子機器７０内の加入者情報にアクセスすることができない。

【０１２０】このように、インターネット３０を介して取得した端末用ＡＰの実行については、携帯電話機５５と電子機器７０との間で上述した一定の条件が成立した場合にのみ実行が許可され、これにより携帯電話機５５から電子機器７０内の加入者情報へのアクセスが可能となる。したがって、携帯電話機５５は、インターネット３０を介して取得したプログラムの実行に際し、セキュリティを確保しつつ、このプログラムに従って当該携帯

電話機５５外の、当該携帯電話機５５と赤外線通信を行うことが可能な電子機器７０内のメモリに記憶されている個人情報にアクセスすることができる。

【０１２１】なお、本実施形態では、携帯電話機５５が電子機器７０との間で赤外線通信を行う場合について説明した。しかしながら、赤外線通信の代わりに、例えば、ＨｏｍｅＲＦや**Bluetooth**（登録商標）を用いてもよい。また、通信ケーブルにより携帯電話機５５と電子機器７０とが有線接続される場合に対しても本発明が適用可能であることは勿論である。

【０１２２】また、アクセス対象は個人情報に限定されず、電子機器７０内のその他の格納データであってもよい。さらに、携帯電話機５５から電子機器７０へのアクセスは、データ以外の、例えば、電子機器７０に格納されているプログラムの起動であってもよい。また、電子機器７０内の入出力ポートへのアクセスなどであってもよい。

【０１２３】［Ｃ．変形例］以上、本発明の実施形態について説明したが、この実施形態はあくまでも例示であり、本発明の趣旨から逸脱しない範囲で様々な変形が可能である。変形例としては、例えば以下のようなものが考えられる。

【０１２４】＜変形例１＞上記第１実施形態では、本体用ＡＰおよびモジュール用ＡＰをコンテンツサーバ２０から一括してダウンロードする場合について説明した。しかしながら、ダウンロードの手順は、例えば、図１２に示されるような手順であってもよい。図１２は、コンテンツサーバ２０からアプリケーションプログラムをダウンロードする場合の変形例について示すシーケンスチャートである。なお、以下の説明では、上記実施形態で述べたダウンロード処理（図９参照）と異なる部分を中心に説明を行う。

【０１２５】同図に示されるように、まず、携帯電話機５０のＣＰＵ５０６は、ダウンロード要求をコンテンツサーバ２０に送信する（ステップＳ３０１）。コンテンツサーバ２０のＣＰＵ２０２は、携帯電話機５０からダウンロード要求を受信すると、このダウンロード要求に応じた本体用ＡＰをＡＰ格納領域２０１ａから読み出す（ステップＳ３０２）。そして、ＣＰＵ２０２は、本体用ＡＰのみを携帯電話機５０にダウンロードする（ステップＳ３０３）。

【０１２６】携帯電話機５０のＣＰＵ５０６は、コンテンツサーバ２０から本体用ＡＰをダウンロードすると、まず、ＪＡＭに従い、ダウンロードした本体用ＡＰの認証処理を行う（ステップＳ３０４）。この認証処理は、例えば、電子署名などによりダウンロードした本体用ＡＰの正当性を確認する処理である。この認証処理の後、ＣＰＵ５０６は、ＪＡＭに従って本体用ＡＰを当該携帯電話機５０に装着されているＵＩＭ６０のモジュールシリアルナンバーと対応付けてＡＰ格納領域５１０ｂに格

納する（ステップＳ３０５）。次いで、ＣＰＵ５０６は、格納した本体用ＡＰに対応するモジュール用ＡＰのダウンロード要求をコンテンツサーバ２０に送信する（ステップＳ３０６）。

【０１２７】コンテンツサーバ２０のＣＰＵ２０２は、携帯電話機５０からのダウンロード要求に応じたモジュール用ＡＰをＡＰ格納領域２０１ａから読み出す（ステップＳ３０７）。そして、ＣＰＵ２０２は、モジュール用ＡＰを携帯電話機５０にダウンロードする（ステップＳ３０８）。

【０１２８】携帯電話機５０のＣＰＵ５０６は、コンテンツサーバ２０からモジュール用ＡＰをダウンロードすると、ＪＡＭに従ってモジュール用ＡＰの認証処理を行う（ステップＳ３０９）。この後、ＣＰＵ５０６は、ＪＡＭに従ってモジュール用ＡＰと当該携帯電話機５０の本体シリアルナンバーとをＵＩＭ６０に送信する（ステップＳ３１０）。

【０１２９】ＵＩＭ６０のＣＰＵ６０４は、モジュール用ＡＰおよび本体シリアルナンバーを受信すると、ＯＳ内のローダに従って、当該モジュール用ＡＰを本体シリアルナンバーと対応付けてＡＰ格納領域５１０ｂに格納する（ステップＳ３１１）。この後、ＵＩＭ６０から携帯電話機５０にインストール完了通知が送信され（ステップＳ３１２）、ダウンロード処理が終了する。

【０１３０】以上説明したようにダウンロード処理は、本体用ＡＰとモジュール用ＡＰとをコンテンツサーバ２０から別々にダウンロードする構成であってもよい。

【０１３１】＜変形例２＞上記第１実施形態および変形例１では、本体用ＡＰおよびモジュール用ＡＰをコンテンツサーバ２０からダウンロードする場合について説明した。しかしながら、本発明は、本体用ＡＰおよびモジュール用ＡＰをコンテンツサーバ２０から各携帯電話機５０に配信する場合についても適用可能である。

【０１３２】この場合、コンテンツサーバ２０は、配信先となる携帯電話機５０の通信アドレス（例えば、ＩＰアドレスやメールアドレスなど）が登録された配信先リストを有する。そして、コンテンツサーバ２０は、送信すべき本体用ＡＰおよびモジュール用ＡＰを上述した配信先リストに登録されている携帯電話機５０およびこれに装着されたＵＩＭ６０に配信する。

【０１３３】＜変形例３＞上記第１実施形態では、アクセス管理処理において、プログラムの実行が指示された本体用ＡＰとこれに対応するモジュール用ＡＰとの認証処理を行うために、本体シリアルナンバーおよびモジュールシリアルナンバーを用いる構成とした。

【０１３４】しかしながら、例えば、コンテンツサーバ２０から本体用ＡＰおよびモジュール用ＡＰを送信する際に、送信するパッケージ毎に異なる識別情報を本体用ＡＰおよびモジュール用ＡＰの両方に付与し、この識別情報を本体シリアルナンバーおよびモジュールシリアルナンバーの代わりに用いる構成としてもよい。

【０１３５】この場合、ダウンロードされた本体用ＡＰやモジュール用ＡＰは、コンテンツサーバ２０によって付与された識別情報と対応付けられて携帯電話機５０のＡＰ格納領域５１０ｂまたはＵＩＭ６０のＡＰ格納領域６０５ｂに格納される。そして、アクセス管理処理において本体用ＡＰとモジュール用ＡＰとの認証処理を行う場合、携帯電話機５０のＣＰＵ５０６は、プログラムの実行が指示された本体用ＡＰに対応付けられている識別情報と、この本体用ＡＰに対応するモジュール用ＡＰに対応付けられている識別情報とが同一であるか否かを照合する。

【０１３６】このような構成とすれば、本体用ＡＰとモジュール用ＡＰとが同一のパッケージでダウンロードされたプログラムであるか否かに基づいて認証を行うことができる。また、本変形例において説明した内容は、ダウンロードの場合のみでなく、配信の場合に対しても適用可能であることは勿論である。

【０１３７】＜変形例４＞上記第１実施形態において、さらに以下に述べる制御を行う構成としてもよい。すなわち、コンテンツサーバ２０は、図１３に示されるように、各本体用ＡＰ毎に、当該本体用ＡＰがＵＩＭ６０内の加入者情報に対して実行可能なアクセス行為を規定したアクセス規定データをメモリ２０１に記憶している。そして、コンテンツサーバ２０は、本体用ＡＰおよびモジュール用ＡＰをダウンロード（または配信）する際に、本体用ＡＰとともにこれに対応するアクセス規定データを携帯電話機５０にダウンロードする。携帯電話機５０では、ダウンロードされた本体用ＡＰとアクセス規定データとを対応付けて不揮発性メモリ５１０に格納する。

【０１３８】そして、携帯電話機５０のＣＰＵ５０６は、アクセス管理処理においてアクセス要求が許容アクセスであるか否かを判別する際に（ステップＳ２１４）、プログラムの実行が指示された本体用ＡＰに対応するアクセス規定データを参照してアクセス要求の可否を決定する。

【０１３９】なお、同図に示されたアクセス規定データにおいて、「可否」項目では、「１」が対応するアクセス行為の許可を、「０」が不許可を示す。また、このアクセス規定データにおけるアクセス行為の可否は、Javaアプレットや**Java**アプリケーションにおける「メソッド」単位で設定される構成であってもよい。例えば、Ａメソッドは許可、Ｂメソッドは不許可など、メソッドの種類に応じてアクセス行為の可否を設定してもよい。

【０１４０】このような構成とすれば、加入者情報に対するアクセスの種類に応じてアクセス要求の可否を決定することができる。

【０１４１】＜変形例５＞上記第１実施形態では、本体用ＡＰの実行が指示されると、当該本体用ＡＰとこれに

対応するモジュール用ＡＰとの認証を行う構成とした。しかしながら、例えば、以下に述べる制御構成であってもよい。

【０１４２】すなわち、携帯電話機５０に対してＵＩＭ６０が装着されると、この時点で、携帯電話機５０に格納されている各本体用ＡＰと、ＵＩＭ６０に格納されている各モジュール用ＡＰとの認証を行い、この携帯電話機５０とＵＩＭ６０の組み合わせにおいて実行可能なアプリケーションプログラム（本体用ＡＰとこれに対応するモジュール用ＡＰ）を特定する構成である。

【０１４３】このように、ＵＩＭ６０が装着された時点で、この携帯電話機５０とＵＩＭ６０の組み合わせにおいて実行可能なアプリケーションプログラムを特定しておく構成とすれば、個々のアプリケーションプログラムの実行が指示された時に、その都度、本体用ＡＰとこれに対応するモジュール用ＡＰの認証を行う必要がない。したがって、アプリケーションプログラムの実行を指示してから当該アプリケーションプログラムが起動するまでの処理が簡素化され、起動時間を短縮できる。

【０１４４】＜変形例６＞上記第１および第２実施形態では、コンテンツサーバ２０は、インターネット３０に接続されている構成とした。しかしながら、このコンテンツサーバ２０は、移動通信網４０の移動パケット通信網内に設置されている構成であってもよい。また、コンテンツサーバ２０は、専用線を介して移動パケット通信網のゲートウェイサーバに直接接続されている構成であってもよい。さらには、このゲートウェイサーバがコンテンツサーバ２０の機能を有する構成であってもよい。

【０１４５】＜変形例７＞上記第１および第２実施形態では、通信端末として携帯電話機５０，５５を用いた場合について説明した。しかしながら本発明は、例えば、移動通信網４０を介してデータ通信を行うことが可能なＰＤＡやモバイルコンピュータなどに対しても適用可能である。また、ＰＨＳ（Personal Handyphone System：登録商標）に対しても適用可能であることは勿論である。また、インターネット３０は、ＬＡＮ（Local Area Network）などのネットワークであってもよい。

【０１４６】＜変形例８＞さらに、図１４に示されるように、通信端末として移動通信網４０を介さずに、インターネット３０のみを介してコンテンツサーバ２０とデータ通信を行うことが可能なパーソナルコンピュータ（以下、パソコンと略称する）８０やサーバ９０などに対しても本発明を適用することが可能である。

【０１４７】図１４に示される例は、パソコン８０からサーバ９０にアクセスする場合について示しており、パソコン８０およびサーバ９０の各々は、インターネット３０を介してデータ通信を行う機能を有している。また、コンテンツサーバ２０には、アクセス元のパソコン８０により実行されるパソコン用ＡＰと、アクセス先のサーバ９０により実行されるサーバ用ＡＰとによって構成されるアプリケーションプログラムが格納されている。

【０１４８】また、パソコン８０は、アクセス先の電子機器（本変形例ではサーバ９０）を特定する情報として、アクセス先となる電子機器の通信アドレス（例えば、ＩＰアドレス）をパソコン用ＡＰと対応付けてメモリに格納する。

【０１４９】本変形例においてパソコン８０およびサーバ９０は、上記第１実施形態において説明したダウンロード処理（図９参照）と同様の処理を実行する。そして、このダウンロード処理においてパソコン８０からの操作入力によって指定されたコンテンツサーバ２０内のパソコン用ＡＰおよびサーバ用ＡＰは、インターネット３０を介してパソコン８０にダウンロードされる。

【０１５０】パソコン８０は、まず、パソコン用ＡＰの送信先となるサーバ９０から当該サーバ９０のシリアルナンバーをインターネット３０経由で取得して、当該シリアルナンバーとダウンロードしたパソコン用ＡＰとを対応付けてメモリに格納する。また、パソコン８０は、サーバ９０の通信アドレスを、このパソコン用ＡＰの処理過程においてアクセスする電子機器の特定情報として、パソコン用ＡＰと対応付けてメモリに格納する。

【０１５１】次いで、パソコン８０は、自機のシリアルナンバーを読み出して、当該シリアルナンバーとダウンロードしたサーバ用ＡＰとをインターネット３０を介してサーバ９０に送信する。サーバ９０では、受信したパソコン８０のシリアルナンバーとサーバ用ＡＰとを対応付けてメモリに格納する。

【０１５２】なお、本変形例においてサーバ用ＡＰは、パソコン８０を経由してサーバ９０にダウンロードされるのではなく、直接、コンテンツサーバ２０からサーバ９０にダウンロードされる形態であってもよい。

【０１５３】そして、パソコン８０およびサーバ９０は、上記第１実施形態において説明したアクセス管理処理（図１０参照）と同様の処理を実行し、プログラムの実行が指示されたパソコン用ＡＰおよびこれに対応するサーバ用ＡＰの相互認証を行う。そして、相互認証されたパソコン用ＡＰおよびサーバ用ＡＰが連携して動作することにより、パソコン８０からサーバ９０に対するアクセスを実現する。

【０１５４】より具体的に説明すると、パソコン８０は、コンテンツサーバ２０からインターネット３０を介して取得したパソコン用ＡＰの実行が指示されると、当該パソコン用ＡＰと対応付けてメモリに格納されている通信アドレスに従って、当該パソコン８０がアクセスするサーバ９０を特定する。

【０１５５】次いで、パソコン８０は、特定したサーバ９０から当該サーバ９０のシリアルナンバーをインターネット３０経由で取得し、パソコン用ＡＰに対応付けられてメモリに格納されているシリアルナンバーと比較す

る。これによりパソコン８０は、現時点においてパソコン８０とインターネット３０を介してデータ通信を行っているサーバ９０がこのパソコン用ＡＰとペアになるサーバ用ＡＰをダウンロードしたサーバ９０であるか否かを判別する。

【０１５６】そして、パソコン８０は、当該パソコン８０とデータ通信を行っているサーバ９０がこのパソコン用ＡＰとペアになるサーバ用ＡＰをダウンロードしたサーバ９０であると判別した場合に、パソコン用ＡＰを実行する。このパソコン用ＡＰによる処理過程においては、パソコン用ＡＰおよびこれに対応するサーバ９０内のサーバ用ＡＰが連携して動作することにより、パソコン８０からインターネット３０を介してサーバ９０へのアクセスが行われる。

【０１５７】つまり、パソコン用ＡＰの実行時において、パソコン８０と通信を行っているサーバ９０がパソコン用ＡＰとペアになるサーバ用ＡＰをダウンロードしたサーバ９０と異なる場合や、このサーバ９０にパソコン用ＡＰに対応するサーバ用ＡＰが格納されていなかった場合などは、パソコン用ＡＰの実行がキャンセルされ、パソコン８０は、サーバ９０にアクセスすることができない。

【０１５８】このように、インターネット３０を介して取得したパソコン用ＡＰの実行については、パソコン８０とサーバ９０との間で上述した一定の条件が成立した場合にのみ実行が許可され、これによりパソコン８０からサーバ９０へのアクセスが可能となる。なお、アクセス対象は、サーバ９０に格納されている個人情報に限定されず、サーバ９０内のその他の格納データであってもよい。さらに、パソコン８０からサーバ９０へのアクセスは、データ以外の、例えば、サーバ９０に格納されているプログラムの起動であってもよい。また、サーバ９０内の入出力ポートへのアクセスなどであってもよい。

【０１５９】したがって、パソコン８０は、インターネット３０を介して取得したプログラムの実行に際し、セキュリティを確保しつつ、このプログラムに従って当該パソコン８０外のリソース、すなわち、当該パソコン８０とインターネット３０を介してデータ通信を行うことが可能な電子機器に格納されているデータへのアクセスやプログラムの起動、入出力ポートへのアクセスなどを行うことができる。

【０１６０】なお、本実施形態において、アクセス元のパソコン８０やアクセス先のサーバ９０は、インターネット３０を介して他のコンピュータとデータ通信を行うことが可能な通信装置であればよく、パソコンやサーバに限定されるものではない。

【０１６１】＜変形例９＞上記第１および第２実施形態では、オープンネットワークを介して組み込まれるプログラムが、Javaアプレットや**Java**アプリケーションなどの**Java**プログラミング言語で記述されたプログラムである場合について説明した。しかしながら、本発明において、**Java**以外のプログラミング言語で記述されたプログラムを本体用ＡＰやモジュール用ＡＰ、電子機器用ＡＰとして用いてもよいことは勿論である。

【０１６２】例えば、図１５に示された本体用ＡＰとモジュール用ＡＰの実行環境を示す機能階層モデルにおいて、本体用ＡＰ「α」は、携帯電話機５０用のＯＳ上で実行されるアプリケーションプログラムであって、ＪＡＭおよび**Java**ＶＭを介さずにＣＰＵ５０６が実行可能である。また、この本体用ＡＰ「α」に対応するモジュール用ＡＰ「α」は、ＵＩＭ６０用のＯＳ上で実行されるアプリケーションプログラムであって、**Java Card** ＶＭを介さずにＣＰＵ６０４が実行可能である。このように、共にＯＳ上で実行される本体用ＡＰ「α」およびモジュール用ＡＰ「α」に対して本発明を適用することも可能である。

【０１６３】＜変形例１０＞上記第１および第２実施形態において、ＵＩＭ６０は、携帯電話機５０，５５などの通信端末と無線通信などによりデータの送受信を行う非接触型のＩＣカードであってもよい。この場合、携帯電話機５０，５５のＵＩＭインタフェース５０５は、当該携帯電話機５０，５５に装着されたＵＩＭ６０との間で無線通信によって行われるデータの送受信を制御する。

【０１６４】

【発明の効果】以上説明したように本発明によれば、通信端末は、セキュリティを確保しつつ、ネットワークを介して得たプログラムに従って当該プログラムのダウンロード元を除く当該通信端末外のリソースにアクセスすることができる。

【図面の簡単な説明】

【図１】　この発明の第１実施形態に係るコンテンツサーバ、携帯電話機およびＵＩＭを含む移動通信システムの構成を例示するブロック図である。

【図２】　同実施形態に係るコンテンツサーバのハードウェア構成を例示するブロック図である。

【図３】　同実施形態に係るコンテンツサーバのＡＰ格納領域の構成を例示する図である。

【図４】　同実施形態に係る携帯電話機のハードウェア構成を例示するブロック図である。

【図５】　同実施形態に係る携帯電話機において、不揮発性メモリのＡＰ格納領域の構成を例示する図である。

【図６】　同実施形態に係るＵＩＭのハードウェア構成を例示するブロック図である。

【図７】　同実施形態に係るＵＩＭにおいて、ＥＥＰＲＯＭのＡＰ格納領域の構成を例示する図である。

【図８】　同実施形態に係る本体用ＡＰとモジュール用ＡＰの実行環境を例示する模式図である。

【図９】　同実施形態に係るコンテンツサーバからアプリケーションプログラムをダウンロードする場合の、コ

33

ンテンツサーバ、携帯電話機およびＵＩＭの動作を例示するシーケンスチャートである。

【図１０】　同実施形態に係る携帯電話機がＵＩＭ内の加入者情報にアクセスする場合の、携帯電話機およびＵＩＭの動作を例示するシーケンスチャートである。

【図１１】　本発明の第２実施形態に係る携帯電話機のハードウェア構成を例示するブロック図である。

【図１２】　変形例１において、コンテンツサーバからアプリケーションプログラムをダウンロードする場合の、コンテンツサーバ、携帯電話機およびＵＩＭの動作を例示するシーケンスチャートである。

【図１３】　変形例４に係るアクセス規定データのデータ構成を例示する図である。

【図１４】　変形例８に係るコンテンツサーバ、パソコンおよびサーバを含む通信システムの構成を例示するブロック図である。

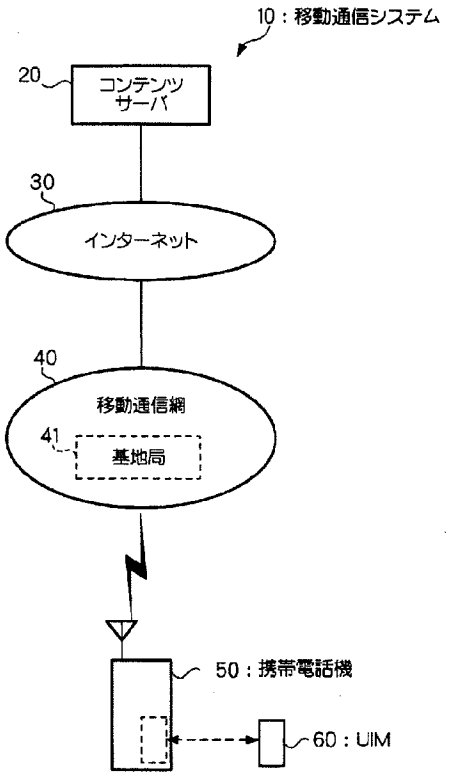
【図１５】　変形例９に係る本体用ＡＰとモジュール用ＡＰの実行環境を例示する模式図である。

【符号の簡単な説明】

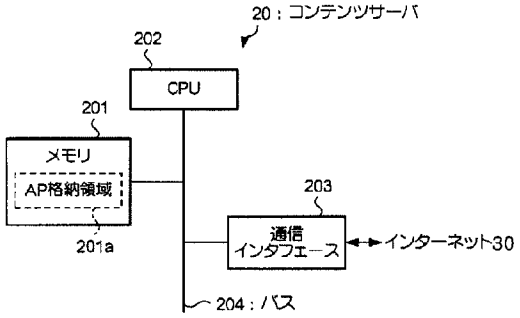
34

１０……移動通信システム、２０……コンテンツサーバ、３０……インターネット、４０……移動通信網、５０，５５……携帯電話機、６０……ＵＩＭ、７０……電子機器、８０……パソコン、９０……サーバ、２０１……メモリ、２０１ａ……ＡＰ格納領域（アプリケーションプログラム格納領域）、２０２……ＣＰＵ、２０３……通信インタフェース、２０４……バス、５０１……無線通信部、５０１ａ……アンテナ、５０２……操作部、５０３……通話処理部、５０４……表示部、５０５……ＵＩＭインタフェース、５０６……ＣＰＵ、５０７……記憶部、５０８……ＲＯＭ、５０９……ＲＡＭ、５１０……不揮発性メモリ、５１０ａ……シリアルナンバー格納領域、５１０ｂ……ＡＰ格納領域、５１１……バス、５５０……赤外線通信部、６０１……外部インタフェース、６０２……ＲＯＭ、６０３……ＲＡＭ、６０４……ＣＰＵ、６０５……ＥＥＰＲＯＭ、６０５ａ……シリアルナンバー格納領域、６０５ｂ……ＡＰ格納領域、６０５ｃ……加入者情報格納領域、６０６……バス。

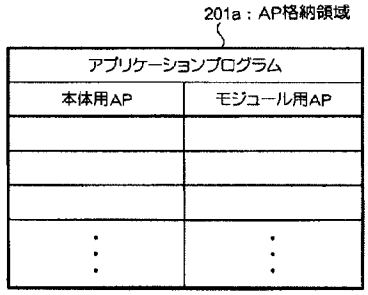
【図１】



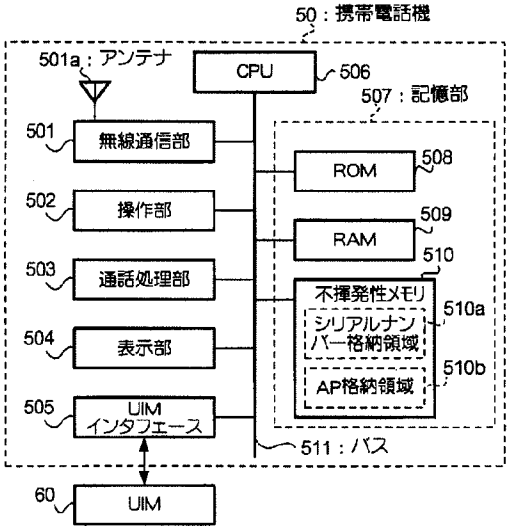
【図２】



【図３】



【図４】

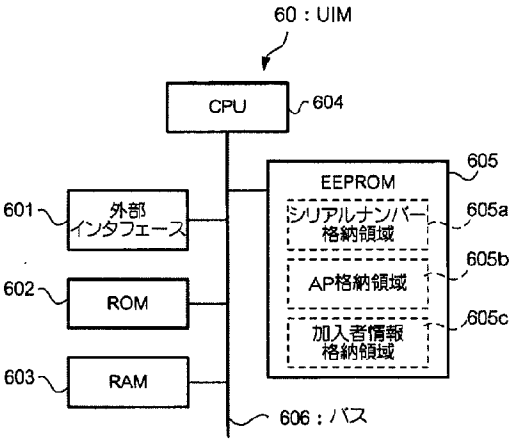


【図５】

510b：AP格納領域

シリアルNo.（UIM）	本体用AP
：	：

【図６】



【図７】

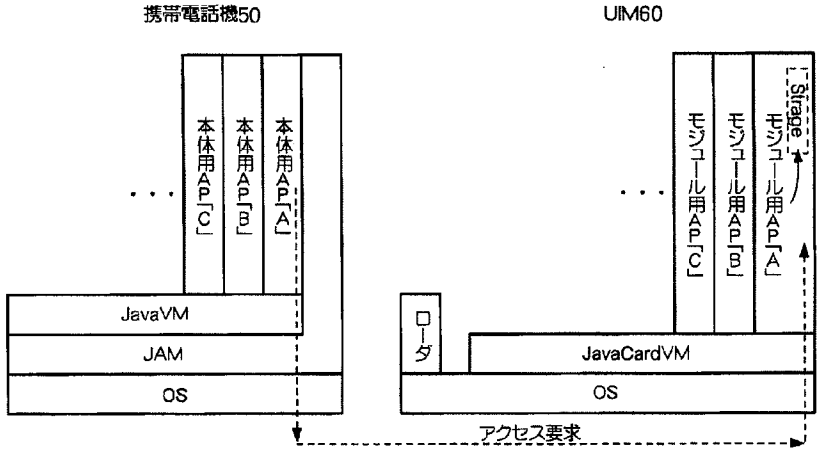
605b：AP格納領域

シリアルNo.（本体）	モジュール用AP
：	：

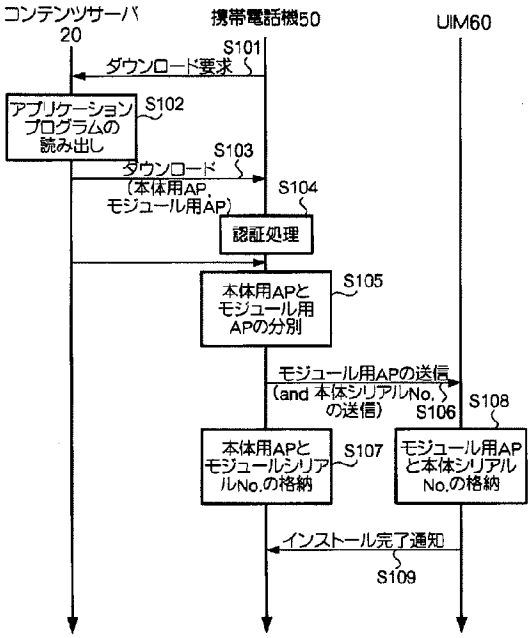
【図１３】

識別情報	アクセス行為	可否
本体用AP「A」	読み出し	1
	書き換え	1
	追加	1
	削除	0

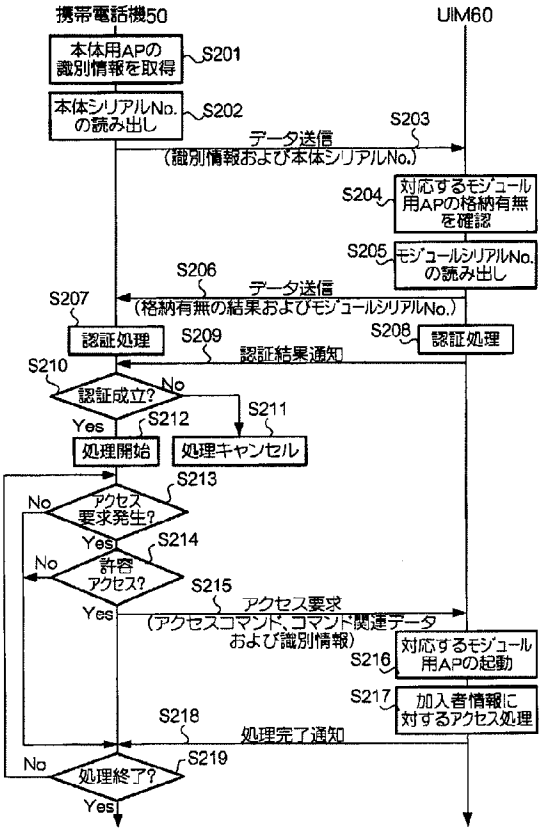
【図８】



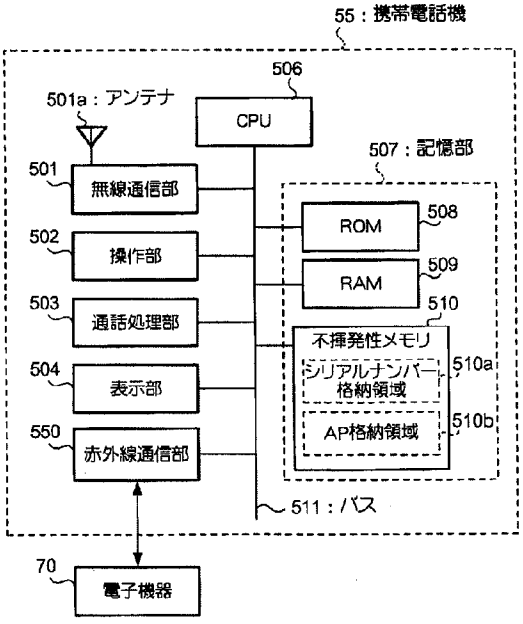
【図９】



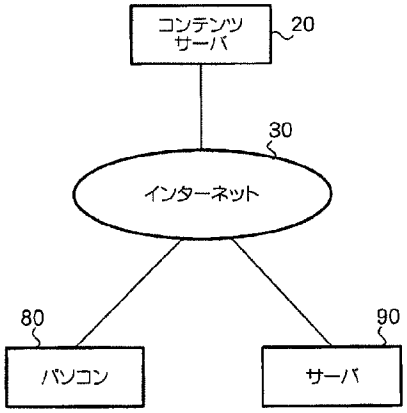
【図１０】



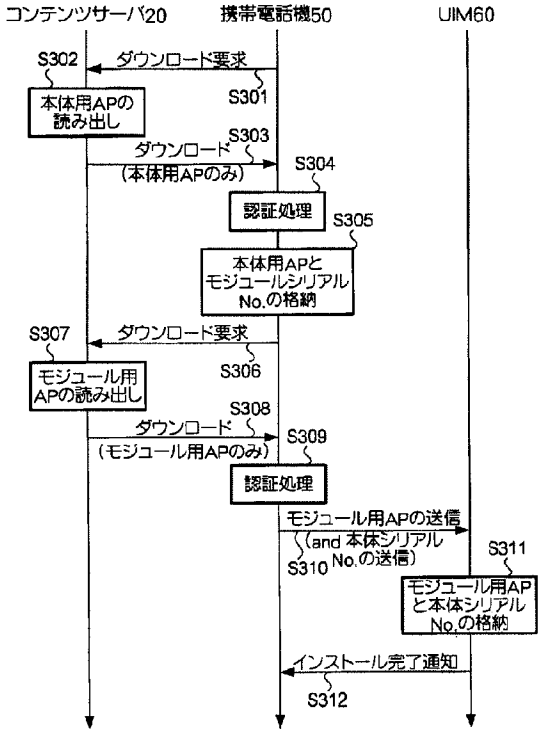
【図１１】



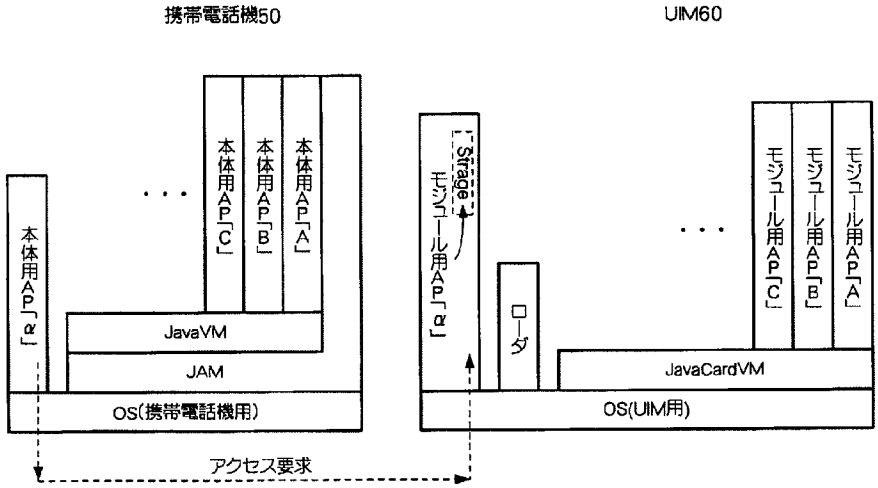
【図１４】



【図１２】



【図１５】



フロントページの続き

(51) Int. Cl.[7]	識別記号	F I		テーマコード（参考）
G06F	15/00	H04M	1/00	V　5K027
H04M	1/00		3/487	
	3/487	G06F	9/06	660G

(72)発明者　東　明洋
東京都千代田区永田町二丁目11番１号　株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　野田　千恵
東京都千代田区永田町二丁目11番１号　株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　古瀬　正浩
東京都千代田区永田町二丁目11番１号　株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　上田　誠
東京都千代田区永田町二丁目11番１号　株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　若林　達明
東京都千代田区永田町二丁目11番１号　株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　平松　孝朗
東京都千代田区永田町二丁目11番１号　株式会社エヌ・ティ・ティ・ドコモ内

Ｆターム(参考)　5B017 AA06 BA09 BB09 BB10 CA15
5B076 BB06 FB02
5B085 AE04 AE12
5K015 AF02 GA01
5K024 AA71 CC11 FF01
5K027 AA11 BB01 CC08 HH26 MM03